EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Cybersecurity Awareness Model with Methods: Analytical Hierarchy Process and Structural Equation Model

Y. Gardenia[1,*] and Alcianno Ghobadi Gani[2]

[1]Air Chief Marshal Suryadarma Aerospace University, Halim Perdanakusuma, Jakarta
[2]Air Chief Marshal Suryadarma Aerospace University, Halim Perdanakusuma, Jakarta

Abstract

This era of revolution has influenced all sectors of society, including education, where technological advancements are now integral to online teaching and learning. However, not everyone fully understands the potential negative impacts of internet usage. The purpose of this research was to investigate and analyze cybersecurity awareness. The study focused on students at Aerospace Air Marshal Suryadarma University. The research employed a quantitative design, either descriptive (where subjects are typically measured once) or experimental (where subjects are measured multiple times). A descriptive study establishes a relationship between variables, while an experimental study determines causation. To analyze the collected data, SEM AMOS was utilized to measure students' awareness of cybersecurity. The study focused on five key areas: (a) regulation, (b) internet usage, (c) password security, (d) data security, and (e) cyberattacks. Based on the research framework and these focus areas, several indicators were developed for the study. The findings concluded that students are aware of cybersecurity issues.

Keywords: Cybersecurity, cybersecurity awareness, structural equation model

Received on 03 06 2024, accepted on 02 07 2024, published on 14 08 2024

doi: 10.4108/eetsis.6931

1. Introduction

Cybersecurity has become a national priority for countries worldwide, including Indonesia. This urgency is driven by the growing integration of information and communication technology across various facets of society, such as law, organization, economy, health, education, culture, security, defense, and more. As the use of information and communication technology increases, the level of threats that can occur is also higher and more complex [1]. In 2022, the National Cyber and Crypto Agency reported 370.02 million cyberattacks in Indonesia [2].

The ongoing revolution of Industry 4.0 and Society 5.0 has significantly contributed to the rise in the number of Internet users. The advanced technology introduced during this era has driven technological development across all aspects of society, including education. Online teaching and learning have greatly benefited from these advancements in Internet technology. However, not everyone is aware of the negative impacts associated with increased Internet use.

According to a survey conducted by the Indonesian Internet Services Association (APJII), Internet penetration in Indonesia has reached 78.19 percent in 2023, a penetration of 215,626.56 of a total population of 275,773,901. The Chief General of APJII noticed this increase. Compared to the previous survey, Indonesia's

[*]Corresponding author. Email: yulisagardenia@gmail.com

internet penetration rate increased by 1.17 percent this year [3].

The behavioral contribution to unintentional cyber breaches was highlighted by IBM's Global Technology Services as one of the most critical issues to be addressed by security controls and best practices guidelines. In fact, there has been an increased recent focus on the role of individual behavior in cyber hazard mitigation. However, the understanding of how individuals differ in their awareness, knowledge, and cybersecurity behavior when confronted with versatile cyber hazards is still quite limited. Moreover, to the best of our knowledge, no research has yet to compare and evaluate these three components across countries [4].

Research conducted by Wijayanto produced a Policy Brief indicating that cybersecurity from the user side is influenced by user password behavior, social media use, access of internet devices and networks, and behavior in accessing information data and using smartphones. These are typical activities often carried out by internet users [5]. Another researcher, Kusumaningrum A. et al., concluded that in general the level of student awareness regarding cybersecurity, especially during the Covid-19 pandemic or when studying from home, was at a "medium" level, with a total score of 79.5%. This figure is close to a good level, and in terms of knowledge, students have a decent grasp at understanding the importance of cybersecurity. All that is required is to familiarize oneself with the cyber security rules [6].

Section 2 reviews literature on cybersecurity, cyber threats, cybercrimes, cyber-attacks, and similar. Section 3 outlines the methodology of our study, explaining the dataset, tools and workflow. Section 4 presents the results through analysis tools: confirmatory factor analysis, validity test, reliability test, and descriptive analysis. Section 5 offers a discussion that provides a deeper understanding of students' awareness and their basic understanding of cybersecurity issues.

This research was conducted to analyze the level of students' awareness of cybersecurity. The author measured the level of awareness and knowledge of cybersecurity among students using the SEM (structural equation model) method, with the aim of seeing the level and extent of such awareness and knowledge.

2. Literature Review

The internet has revolutionized how people access data and utilize various applications for modern day-to-day tasks. Reid and Van Niekerk [7] noted the huge impact of the internet on daily life: "In our technology and information-infused world, cyberspace is an integral part of the modern-day society."

In both personal and professional contexts, cyberspace is a highly effective tool in, and enabler of, most people's daily digitally transposed activities [8]. Individual cyber engagement, in general, and cyber protection tools in particular, have motivated both academic scholars and practitioners to focus on individual attitudes and behavior concerning cyber threats [9]. Other studies have evaluated the level of individual resilience related to cybersecurity awareness in regard to it being a cause of job stress [10]. In addition, the relationship between individual personality and level of cybersecurity risk propensity has been researched [10]. Yet the relationships between individual cyber security awareness, and knowledge and behavior have never been studied in cross-country comparison, yet the comparative approach is considered by important stakeholders to be crucial for the creation of intervention programs [10].

The International Telecommunications Union (ITU) defines cybersecurity as follows: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and an organization and user's assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity - which may include authenticity and nonrepudiation - and confidentiality [11].

Cybersecurity awareness can be defined as when a person has a good knowledge or ability to practice security when using internet networking sites and when they understand the importance of protecting personal data and/ or group data in the name of an organization when deciding to use a web site [12]. Knowledge about cybersecurity awareness or cybersecurity is very necessary at this time for organizations, companies or individuals when using the internet to avoid interference, cyber threats or cyber attacks which could occur at any time. Expanding the horizons of a person's cyber security awareness, such as protecting personal information or data and maintaining device security, for example via password usage, can minimize the risk of interference, threats and attacks.

Cybercrimes can be defined as violations committed against individuals or groups of individuals with criminal motives to deliberately hurt the victim's reputation or cause physical or mental harm to victims directly or indirectly, using modern telecom networks such as the Internet (included but not limited to chat rooms, email, bulletin boards and groups) and cell phones [13]. Table 1 presents different categories of cybercrime.

Table 1. Different Categories Of Cybercrime [14,15]

Category	Definition
Hacking	The destruction and concealment of information from the victim's operating system by attacking the weaknesses and loopholes are known as hacking. It is usually done by installing some sort of backdoor programs by hackers on the computer of victims to obtain access to the information.
Cyber theft	When the victim's computer information is stolen through electronic attacks, this is known as cyber theft. The most common example of cyber theft is credit card fraud and illegal money transfers.
Viruses and worms	Viruses and worms are designed to damage the computers attached to other programs and documents in the computer. They appear to perform some other function, but the primary function of the virus is to corrupt the operating system of the computer.
Spamming	Spamming is done by sending massive numbers of emails to users that usually contain links designed to harm the programs of the victim's computer.
Financial fraud	This cybercrime is also known as a phishing scam, formed through social engineering and designed to obtain the victim's bank details.
Identity theft and credit card theft	In this cybercrime, emails are sent to users to induce them to provide their identity card and credit card information. The attacker represents him or herself as a representative of some well-known company, and hence unaware users provide their sensitive details by responding to these emails.
Cyber harasment	Cyber harassment is harassing and bullying individuals using electronic means; one such example is cyberstalking.
Cyber laundring	The transfer of illegally obtained money between two parties is known as cyber laundering.
Website cloning	Copying the websites of renowned companies and attacking the users who are unaware of this is a new category of cybercrime. Unaware consumers provide their details to the fraudster's personal database.

3. Methodology

This study used a quantitative research technique to emphasize students' cyber security awareness. Quantitative research designs are either descriptive (in which subjects are generally measured just once) or experimental (subjects are measured many times). A relationship between variables is established in a descriptive investigation; causation is established in an experimental study.

To analyse the collected data, SEM AMOS was utilized to measure students' awareness of cyber security. SEM is an integrated approach between two analyses, namely factor analysis and path analysis. S. Y. Lee [16] stated that structural equation models are well recognized as the most important statistical method to serve the above purpose and can be applied to many fields. SEM uses statistical methods to present data in achieving research objectives and can apply various models to achieve research objectives and answer research problem formulations [17].

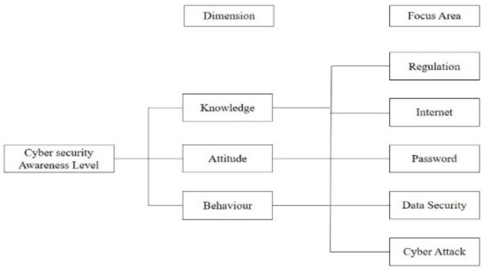

Figure 1. Research Framework of Cyber Security

There were a total of 5 focus areas used: (a) regulation, (b) internet, (c) password, (d) data security, and (e) cyber attack. From the research framework and specified focus areas above, several indicator questions were made for this research.

Questionnaires were distributed by online link to Unsurya students and the online link was sent to students' whatsapp group; the design used a Likert scale of 1 to 5 (Table 2). The concept of the measurement framework for cybersecurity awareness, introduced by Krugger & Kerney, evaluates the level of student cybersecurity awareness based on three dimensions of knowledge, attitude and behavior [18].

Table 2. Questions from each dimension

No	Knowledge	Attitude	Behavior
1.	Know about regulation	be careful in post someting	never post hoax
2.	Know about data security	using antivirus on laptop and gadget	always act carefully when sent something
3.	know whats strong password look like	use secure passwords for all the applications I have	never share password to someone
4.	know the internet and the dangers of using the internet	use many applications on gadgets and laptops	downloaded safe apps
5.	know about cybercrime	keep my personal username and password	never hacked other people's social media or emails

4. Result

The SEM model in this research sample has a number of latent variables (constructs) of up to five, and each construct is explained by three or more indicators, a sample size of 100-150 data is considered adequate [19]. Table 3 shows the demographics of the survey participants, revealing that the male population (80.4%) was somewhat greater than the female population (10.68%).

Table 3. Respondent Details

Variable	Group	Frequency	Percentange(%)
Gender	Male	82	80,4%
	Female	20	19,6%
	Total	**102**	**100%**
Major	Aeronautical Engineer	76	74,5%
	Aeronautic	5	4.9%
	AMTO	14	13,7%
	ATC	7	6.9%
	Total	**102**	**100%**

The processing tool uses Structural Equation Modeling (SEM) using the AMOS (Analysis of Moment Structure) program version 26. Prior to data analysis, validity and reliability tests of the questionnaire used are performed. To measure its validity, the score of each question item was used, which was correlated with the total item score in one variable [20]. After testing the validity and reliability, data analysis was performed. Data analysis and interpretation are carried out to answer the problems formulated and respond to the hypotheses. The stages of data processing were as follows: Assessing Goodness-of-Fit Criteria, RMSEA (The root Mean Square Error of Approximation), GFI (Goodness of Fit Index), NFI (Normed Fit Index) and hypothesis testing. The hypothesis would be accepted with a value of β> 0, where β is the estimated parameter value and the value of P<0.1 [21].

The research model's variables could be used in other similar research with different data, although a successful goodness-of-fit does not necessarily mean that the model is valid. It is a useful indicator, however, to move forward with further procedures to calculate the structured validity [23]. The number of variables (factors) in the measurement model has an impact on the model fit values; the simpler the model and the fewer variables it has, the higher the possibility of getting better model fit values; also, the normality of the collected data indicates a possibility of getting a better model fit [23].

Factor loading between the latent variable (construct) and its related observed variable (items) is used to estimate their relationship. High loading was expected to be found, as represented by the standardized loadings estimates, and should be between 0 and 1. Factor loading with results more than 0.5 and less than 0.7 can be taken into consideration if this does not affect reliability and validity negatively; an item with a loading less than 0.5 was to be removed from the model. A factor loading of around 0.7 or more can be considered an ideal loading that indicates a strong relationship; however, a factor loading of 1 or more can indicate some problems with collected data [24].

4.1 Validity and Reliability Test

Table 4. Reliability Test

			Estimate
k1	<---	Knowledge	,437
k2	<---	Knowledge	,659
k3	<---	Knowledge	,650
k4	<---	Knowledge	,579
k5	<---	Knowledge	,573
a5	<---	Atittude	,462
a4	<---	Atittude	,267
a3	<---	Atittude	,652
a2	<---	Atittude	,612
a1	<---	Atittude	,382
b1	<---	Behavior	,482
b2	<---	Behavior	,667
b3	<---	Behavior	,588
b4	<---	Behavior	,697
b5	<---	Behavior	,362

Table 5. Validity Reability Test

			Estimate	S.E.	C.R.	P	Label
Knowledge	<-->	Behavior	,149	,048	3,075	,002	
Knowledge	<-->	Atittude	,151	,048	3,140	,002	
Atittude	<-->	Behavior	,174	,053	3,284	,001	
			Estimate	**S.E.**	**C.R.**	**P**	**Label**
Knowledge	<-->	Behavior	,149	,048	3,075	,002	
Knowledge	<-->	Atittude	,151	,048	3,140	,002	
Atittude	<-->	Behavior	,174	,053	3,284	,001	

4.2 Hypotheses testing

Hypothesis testing can be made after making sure the collected data fits the research model and an appropriate R2 is acquired. The probability P-value is calculated in this step to see whether or not to accept the hypothesis [25]; a P-value of 0.05 or less is an indicator to accept the hypothesis [24]. When conducting path analysis for hypotheses testing, standardized and unstandardized paths are calculated. The standardized paths, however, are used when reporting the results (Valenzuela, 2017).

Research hypothesis:
H1: Knowledge has a positive and significant effect on SMEs attitude and behavior.
H2: Attitude has a positive and significant effect on SMEs knowledge and behavior.
H3: Behavior has a positive and significant effect on SMEs attitude and knowledge.

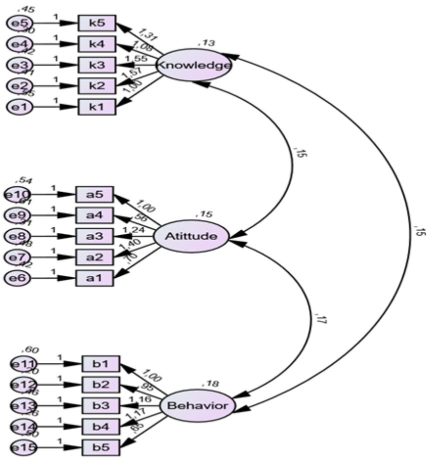

Figure 2. AMOS Result Analysis

5. Conclusion

The purpose of this research was to look into and analyse cyber security concern in Aerospace Air Marshal Suryadarma University. According to the conclussions of this survey, students are aware of cybersecurity. Based on hypothesis knowledge has a positive and significant effect on SMEs attitude and behavior, attitude has a positive and significant effect on SMEs knowledge and behavior, behavoiur has a positive and significant effect on SMEs attitude and knowledge. Much more research is needed to establish how students' knowledge levels might be increased by implementing appropriate awareness-raising initiatives. Further research may be needed to identify how best practices might improve the issue areas identified in this study [15].

Acknowledgements.

We would like to thank the Air Chief Marshal Suryadarma University for allowing us to conduct research. Thanks to all students who have helped fill in the questionnaire and we would also like to thank all those who have helped us complete this research.

Appendix A

Structural equation modeling (SEM) is a powerful statistical technique that goes beyond traditional regression analysis. It allows researchers to explore complex relationships between observed variables and underlying, latent constructs that cannot be directly measured [26]. SEM integrates aspects of:

1. Factor analysis: Identifies underlying factors (latent constructs) from a set of observed variables.
2. Regression analysis: Examines how one set of variables (independent) predicts another (dependent) [27].

Key concepts in SEM:

- Latent variables (constructs): Underlying factors that represent abstract concepts, not directly measurable (e.g., intelligence, customer satisfaction).
- Observed variables (indicators): Measurable variables that reflect the latent constructs (e.g., test scores, customer survey responses).
- Structural model: Represents the hypothesized relationships between latent and observed variables, including direct and indirect effects.
- Measurement model: Defines how the latent constructs are measured by the observed variables.

Result- Goodness of Fit Index CFA

Goodness of Fit Index	cut off value	Result	Criteria
Chi-Square	< 18947.21	213,111	Fit
DF	> 0	87	Good Fit
Probability	> 0,05	0,000	Moderat
CMIN/DF	< 5	2,450	Fit
GFI	≥ 0,90	0,785	Good Fit
RMSEA	≤ 0,08	0,100	Moderat
AGFI	≥ 0,90	0,703	Moderat
TLI	≥ 0,90	0,691	Moderat
NFI	≥ 0,90	0,643	Moderat
CFI	≥ 0,90	0,744	Moderat
PNFI	≥ 0,60	0,533	Moderat
PGFI	≥ 0,60	0,569	Good Fit

Appendix B

The Covariance Matrix

Covariance between constructs— Covariance is the measure of how much two variables change together. If greater values of one variable correspond to greater values of another variable, you have a positive covariance. If greater values in one variable correspond to lower values of another variable, there is a negative covariance value. The main function of covariance analysis is to determine the directionality of two variables. If the covariance is positive, then the two variables will move in the same direction. If the covariance is negative, the two variables will move in opposite directions. One of the primary assumptions in SEM is that the relationship between constructs follows a linear pattern. Put another way, if a scatter plot of the values of two variables is ran, then the data would lie in a linear pattern that increased upward or decreased downward [20].

The covariance formula is:
For a population:

$$Cov(x,y) = \frac{\Sigma\,(\mathrm{x}_1-\bar{\mathrm{x}})(y_1-\bar{y})}{n} \tag{B.1}$$

For a sample of the population :

$$Cov(x,y) = \frac{\Sigma\,(\mathrm{x}_1-\bar{\mathrm{x}})(y_1-\bar{y})}{n-1} \tag{B.2}$$

References

[1] H. Siburian, “Strategy of Cyber Security,” *BSSN*, 2023. https://www.bssn.go.id/strategi-keamanan-siber-nasional/.

[2] BPPTIK, “Statistical Data,” 2023. www.bpptik.kominfo.go.id.

[3] S. R. Puspita, “APJII : Survei Penetrasi Internet Indonesia 2024,” 2024. [Online]. Available: https://www.cloudcomputing.id/berita/apjii-survei-penetrasi-internet.

[4] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, “Cyber Security Awareness, Knowledge and Behavior: A Comparative Study,” *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.

[5] M. Ulum and U. M. Jakarta, “Policy Brief Recommendation: Cyber Security and Defence Policy of Indonesia,” no. July, pp. 0–6, 2018, doi: 10.13140/RG.2.2.28227.09763.

[6] A. Kusumaningrum, H. Wijayanto, and B. D. Raharja, “Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA),” *J. Ilm. SINUS*, vol. 20, no. 1, p. 69, 2022, doi: 10.30646/sinus.v20i1.586.

[7] R. Reid and J. Van Niekerk, “Decoding audience interpretations of awareness campaign messages,” *Inf. Comput. Secur.*, vol. 24, no. 2, pp. 177–193, Jan. 2016, doi: 10.1108/ICS-01-2016-0003.

[8] F. Mokrini, L. Waeyenberge, N. Viaene, and M. Moens, “First Report of the Cereal Cyst Nematode Heterodera latipons on Wheat in Morocco,” *Plant Dis.*, vol. 96, no. 5, p. 774, Feb. 2012, doi: 10.1094/PDIS-11-11-0999-PDN.

[9] J. Shropshire, M. Warkentin, A. Johnston, M. Schmidt, A. C. Johnston, and M. B. Schmidt, “Association for Information Systems AIS Electronic Library (AISeL) Personality and IT security: An application of the five-factor model Recommended Citation Mark, ‘Personality and IT security: An application of the five-factor model’ Personality and IT security: An application of the five-factor model,” p. 415, 2006, [Online]. Available: http://aisel.aisnet.org/amcis2006/415.

[10] A. McCormac, D. Calic, K. Parsons, M. Butavicius, M. Pattinson, and M. Lillie, “The effect of resilience and job stress on information security awareness,” *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 277–289, Jan. 2018, doi: 10.1108/ICS-03-2018-0032.

[11] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[12] O. Rokhman *et al.*, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” *J. Berk. Epidemiol.*, vol. 5, no. 1, pp. 90–96, 2020, [Online]. Available: https://core.ac.uk/download/pdf/235085111.pdf%250A website: http://www.kemkes.go.id%250Ahttp://www.yankes.kemkes.go.id/assets/downloads/PMK No. 57 Tahun 2013 tentang PTRM.pdf%250Ahttps://www.kemenpppa.go.id/lib/uploads/list/15242-profil-anak-indonesia_-2019.pdf%25.

[13] A. G. Gani, “Cybercrime (Kejahatan Berbasis Komputer),” *J. Sist. Inf. Univ. Suryadarma*, vol. 5, no. 1, pp. 16–29, 2014, doi: 10.35968/jsi.v5i1.18.

[14] I. Frank and E. Odunayo, “Approach to cyber security issues in nigeria: Challenges and solution,” *Int. J. Cogn. Res. Sci. Eng. Educ.*, vol. 1, no. 1, 2013.

[15] L. Alzahrani, “Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 11, pp. 630–637, 2021, doi: 10.14569/IJACSA.2021.0121172.

[16] S. Y. Lee, *Structural Equation Modelling*. 2007.

[17] R. B. Kline, “Response to Leslie Hayduk’s review of principles and practice of structural equation modeling,1 4th edition,” *Can. Stud. Popul.*, vol. 45, no. 3–4, pp. 188–195, 2018, doi: 10.25336/csp29418.

[18] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006, doi: https://doi.org/10.1016/j.cose.2006.02.008.

[19] S. Santoso, *Application SEM Amos 22*. 2014.

[20] J. E. Collier, “Applied Structural Equation Modeling Using AMOS,” *Appl. Struct. Equ. Model. Using AMOS*, 2020, doi: 10.4324/9781003018414.

[21] A. Purwanto, A. Sulaiman, and K. Fahmi, “The Role of Buzz and Viral Marketing on SMEs Online Shop Marketing Performance: CB-SEM AMOS Analysis,” *Int. J. Soc. Manag. Stud.*, vol. 4, no. 3, pp. 1–7, 2023.

[22] B. M. Byrne, “Structural equation modeling with AMOS: Basic concepts, applications, and programming, 2nd ed.,” *Structural equation modeling with AMOS: Basic concepts, applications, and programming, 2nd ed.* Routledge/Taylor & Francis Group, New York, NY, US, pp. xix, 396–xix, 396, 2010.

[23] M. YAŞLIOĞLU and D. TOPLU YAŞLIOĞLU, “How and When to Use Which Fit Indices? A Practical and Critical Review of the Methodology,” *Istanbul Manag. J.*, pp. 1–20, 2020, doi: 10.26650/imj.2020.88.0001.

[24] J. F. Hair Jr, *Multivariate data analysis*. 2014.

[25] de J. Carvalho and O. F. Chima, “Applications of Structural Equation Modeling in Social Sciences Research,” *Am. Int. J. Contemp. Res.*, vol. Vol. 4, no. 1, pp. 6–11, 2014.

[26] T. N. Beran and C. Violato, “Structural equation modeling in medical,” *BMC Res. Notes*, vol. 3, no. 267, pp. 1–10, 2010, [Online]. Available: http://www.biomedcentral.com/1756-0500/3/267.

[27] “Structural Equation Modeling.” https://www.statisticssolutions.com/free-resources/directory-of-statistical-analyses/structural-equation-modeling/.