Sage Science Review of Educational Technology
- ✓ G21: Banks; Other Depository Institutions; Micro Finance Institutions; Mortgages
- ✓ G28: Government Policy and Regulation
- ✓ C21: Cross-Sectional Models; Spatial Models; Treatment Effect Models; Quantile Regressions
- ✓ C52: Model Evaluation, Validation, and Selection
- ✓ D83: Search; Learning; Information and Knowledge; Communication; Belief; Unawareness

Understanding Security Awareness Among Bank Customers: A Study Using Multiple Regression Analysis

Joan Telo

Abstract

Background: The banking industry has witnessed a significant rise in cyber-attacks, in recent decades, making it necessary for banks to implement effective security measures to safeguard their customers' information. One key aspect of ensuring information security is to increase customers' security awareness.

Objective: This study aims to identify the factors that significantly impact the security awareness of bank customers using a dataset of 477 customers of different ages.

Methods: The study employs multiple regression analysis with HAC standard errors to examine the relationship between seven independent variables (Age and Experience, Education and Awareness Programs, User Experience, Cyber Threat Landscape, Trust in the Bank, Personal Factors, Convenience) and the dependent variable, security awareness.

Results: The findings indicate that all seven independent variables have a significant impact on the security awareness of bank customers at a 10 percent significance level. However, personal factors and Cyber Threat Landscape are insignificant at a 1 percent level of significance.

Conclusion: The study argues that banks need to take into account all seven independent variables when designing strategies to increase the security awareness of their customers. While personal factors and Cyber Threat Landscape may not have a significant impact individually, they still need to be considered as part of a holistic approach to information security. The insignificant results of personal factors and Cyber Threat Landscape could be due to the complexity of the constructs or the limited sample size. Further research with larger samples could help to provide a more nuanced understanding of these variables' impact on customers' security awareness.

Keywords:

1. *Bank customers*
2. *Cybersecurity*
3. *Independent variables*
4. *Multiple regression*
5. *Security awareness*

Date of Submission: March 14, 2022
Date of Peer Review: April 17, 2022
Date of Acceptance: Nov 19, 2022
Month of Publishing: February 2023
Financial or other competing interests: non

Introduction

Cyber-attacks have become increasingly common, in modern world, posing a significant threat to individuals, businesses, and governments alike. With the increasing reliance on technology, cyber threats have evolved to become more sophisticated and complex, making it challenging for organizations to protect themselves. Cybersecurity has become an essential aspect of the digital age, and the need for effective measures to counter cyber threats has become a critical concern for many. Cyber-attacks are intentional acts of malicious individuals or groups to compromise computer systems, networks, or devices to gain unauthorized access or damage them. Cybercriminals use various methods, such as malware, phishing, social engineering, and denial-of-service (DoS) attacks, to infiltrate systems and extract sensitive data or cause disruption. The impact of cyber-attacks can be devastating, causing financial losses, reputational damage, and even endangering lives in some cases.

One of the significant cyber threats that organizations face is ransomware attacks. Ransomware is a type of malware that encrypts files and demands payment in exchange for the decryption key. Ransomware attacks have become more prevalent in recent years, with cybercriminals targeting companies and organizations of all sizes. In many cases, organizations opt to pay the ransom to regain access to their data, which encourages cybercriminals to continue with their activities.

Phishing is another common cyber threat that targets individuals and organizations. Phishing attacks involve the use of fraudulent emails or websites to trick users into providing personal or sensitive information, such as login credentials or financial details. Cybercriminals can then use this information to carry out further attacks or sell the data on the dark web. Phishing attacks have become increasingly sophisticated, with attackers using advanced techniques, such as spear-phishing and whaling, to target specific individuals or organizations. Social engineering is another tactic used by cybercriminals to gain access to systems or data. Social engineering involves manipulating individuals to divulge sensitive information or perform actions that could compromise their systems. Attackers use various techniques, such as pretexting, baiting, or quid pro quo, to trick individuals into revealing information or clicking on malicious links.

Denial-of-service (DoS) attacks are another type of cyber threat that targets systems or networks. DoS attacks involve flooding a system with traffic to overwhelm it and cause it to crash or become unavailable. DoS attacks can have severe consequences, particularly for organizations that rely on their systems or networks to provide critical services. Distributed denial-of-service (DDoS) attacks, which involve using multiple systems to launch the attack, have become more prevalent in recent years, making it more challenging to defend against them.

Cybersecurity is a crucial aspect of the banking industry, given the critical nature of the industry and the value of the information and assets it handles. With the increasing use of digital technologies in banking, such as online banking, mobile banking, and electronic payments, cyber threats have become more prevalent and sophisticated. This article will explore the importance of cybersecurity in the banking industry, the challenges it faces, and the measures that banks can take to enhance their cybersecurity.

The banking industry is a prime target for cybercriminals, given the high-value assets and sensitive information that it handles. A successful cyber-attack on a bank can result in financial losses, damage to the bank's reputation, and a loss of customer trust. Moreover, cyber-attacks on the banking industry can have broader implications for the economy, as the industry plays a critical role in the functioning of financial systems.

In addition to traditional financial crimes such as fraud and embezzlement, cybercriminals target banks for a range of reasons, such as stealing sensitive information, disrupting operations, and using bank systems as a gateway to attack other organizations. Cyber-attacks on banks can take various forms, such as phishing attacks, malware attacks, ransomware attacks, and Distributed Denial of Service (DDoS) attacks.

The banking industry faces various challenges in enhancing its cybersecurity, such as the increasing complexity of the technology landscape, the sophistication of cyber threats, and the need to balance security with customer convenience. Banks must also comply with a range of regulatory requirements related to cybersecurity, such as the Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLBA), and the General Data Protection Regulation (GDPR).

One of the most significant challenges that banks face is the increasing complexity of the technology landscape. Banks use a wide range of technologies to deliver services to customers, such as mobile apps, online banking portals, and ATMs. Each of these technologies presents unique security risks that banks must manage. Moreover, banks must ensure that these technologies are integrated seamlessly and securely to deliver a consistent customer experience.

The sophistication of cyber threats is also a significant challenge for the banking industry. Cybercriminals use increasingly sophisticated methods to breach banks' security defenses, such as social engineering tactics, zero-day exploits, and advanced malware. These attacks can be difficult to detect and can cause significant damage to banks' systems and reputation.

The need to balance security with customer convenience is another challenge for banks. While robust security measures are necessary to protect against cyber threats, customers also expect convenience and ease of use when accessing banking services. Banks must find ways to strike a balance between security and convenience, such as using multi-factor authentication and risk-based authentication to reduce the friction of security measures.

Security awareness of online banking customers is critical in today's digital age. As more customers adopt online banking, the risk of cyber threats and attacks on online banking systems increases. Customers who lack security awareness may be vulnerable to phishing scams, malware attacks, and other cyber threats that can lead to financial losses, identity theft, and other negative consequences. In this article, we will discuss the importance of security awareness for online banking customers, the challenges they face, and the measures they can take to enhance their security awareness.

The importance of security awareness for online banking customers cannot be overstated. With the increasing use of digital technologies in banking, such as online banking portals, mobile banking apps, and electronic payments, cyber threats have

become more prevalent and sophisticated. Customers who lack security awareness may fall prey to phishing scams and other social engineering tactics that can result in the compromise of their accounts, theft of personal information, and financial losses.

Moreover, the consequences of a cyber attack on an online banking customer can be significant. A compromised account can result in unauthorized transactions, fraudulent withdrawals, and other financial losses. Moreover, identity theft can have long-lasting consequences, such as damage to credit scores, difficulty obtaining credit or loans, and other negative impacts.

Challenges faced by online banking customers in enhancing their security awareness

Online banking customers face various challenges in enhancing their security awareness, such as the increasing sophistication of cyber threats, the need to balance security with convenience, and the lack of awareness of cybersecurity best practices.

The increasing sophistication of cyber threats is one of the significant challenges faced by online banking customers in enhancing their security awareness. Cybercriminals use a range of tactics to deceive customers and gain access to their accounts, such as phishing emails, fake websites, and social engineering tactics. These attacks can be difficult to detect, and customers may inadvertently provide sensitive information to cybercriminals. The need to balance security with convenience is another challenge faced by online banking customers. While robust security measures are necessary to protect against cyber threats, customers also expect convenience and ease of use when accessing banking services. Customers may be reluctant to adopt security measures that add friction to their banking experience, such as multi-factor authentication or complex passwords. Finally, the lack of awareness of cybersecurity best practices is another challenge faced by online banking customers. Many customers may not be aware of the risks associated with online banking, such as the importance of creating strong passwords, avoiding phishing scams, and keeping their devices up to date with security patches.

Hypotheses

Age and Experience:

Null hypothesis: Age and experience do not affect the security awareness of online banking customers.

Alternative hypothesis: Younger and more experienced online banking customers have a higher level of security awareness compared to older and less experienced customers.

Education and Awareness Programs:

Null hypothesis: The availability and effectiveness of education and awareness programs do not have a significant impact on the security awareness of online banking customers.

Alternative hypothesis: The availability and effectiveness of education and awareness programs can increase the security awareness of online banking customers and improve their ability to protect themselves against potential risks.

User Experience:

Null hypothesis: The user experience of online banking platforms does not influence the security awareness of online banking customers.

Alternative hypothesis: If online banking platforms provide an easy and intuitive user experience, customers are more likely to use them correctly and be aware of potential security risks.

Cyber Threat Landscape:

Null hypothesis: The cyber threat landscape does not affect the security awareness of online banking customers.

Alternative hypothesis: High-profile cyber attacks and data breaches can increase the security awareness of online banking customers and encourage them to take additional security measures.

Trust in the Bank:

Null hypothesis: The level of trust that customers have in their bank does not affect their security awareness.

Alternative hypothesis: If customers trust their bank to protect their personal and financial information, they may be less likely to take additional security measures themselves.

Personal Factors:

Null hypothesis: Personal factors such as age, education level, and technical proficiency do not affect the security awareness of online banking customers.

Alternative hypothesis: Personal factors such as age, education level, and technical proficiency can play a significant role in determining the level of security awareness among online banking customers.

Convenience:

Null hypothesis: Convenience does not affect the security awareness of online banking customers.

Alternative hypothesis: Customers who prioritize convenience may be more likely to overlook security risks or take shortcuts, such as using simple passwords or accessing online banking on public Wi-Fi networks.

Methodology

Following the discussion above and, specifically, the hypotheses section, we formulated the multiple regression as follows:

$$SA = \alpha + \beta_1 Age_i + \beta_2 edu_i + \beta_3 \exp r_i + \beta_4 cyber_i + \beta_5 Trust_i + \beta_6 Personal_i + \beta_7 Conv_i + \varepsilon_i$$

Where, SA denotes the Security Awareness Index. The descriptions of the independent variables are provided in table 1.

Table 1. Independent variables

Factors	Symbol	Impact on Security Awareness of Online Banking Customers
Age and Experience	*Age*	Younger customers may have a greater understanding of online security, while older customers may be less familiar with online threats. Customers who have been using online banking for a longer time may also have a better understanding of potential risks.
Education and Awareness Programs	*Edu*	The availability and effectiveness of education and awareness programs can play a significant role in increasing security awareness among online banking customers. Banks and financial institutions should invest in creating awareness programs to educate customers about the risks associated with online banking and how to protect themselves.
User Experience	*expr*	The user experience of online banking platforms can influence the security awareness of customers. If online banking platforms are easy to use, intuitive, and provide clear instructions and guidance, customers are more likely to use them correctly and be aware of the potential risks.
Cyber Threat Landscape	*Cyber*	High-profile cyber attacks and data breaches can increase awareness among customers and encourage them to take additional security measures.
Trust in the Bank	*Trust*	The level of trust that customers have in their bank can impact their security awareness. If customers trust their bank to protect their personal and financial information, they may be less likely to take additional security measures themselves.
Personal Factors	*Personal*	Personal factors such as age, education level, and technical proficiency can play a role in determining the level of security awareness among online banking customers. Younger, more tech-savvy individuals may be more aware of the potential risks associated with online banking, while older individuals or those with less technical expertise may require additional education and support.
Convenience	*conv*	Customers who prioritize convenience may be more likely to overlook security risks or take shortcuts, such as using simple passwords or accessing online banking on public Wi-Fi networks.

Results

Table 2 shows the output from a multiple regression analysis with the dependent variable SA and seven independent variables: AGE, CONV, CYBER, EDU, EXPR, PERSONAL, and TRUST, as well as a constant term (C). The coefficient for each

independent variable represents the estimated effect of that variable on the dependent variable, holding all other variables constant. The standard error is a measure of the uncertainty in the estimated coefficient, and the t-statistic tests the null hypothesis that the true coefficient is zero. The associated p-value indicates the probability of observing a t-statistic as large or larger than the observed value, assuming the null hypothesis is true. Based on this output, we can see that all the independent variables except PERSONAL have statistically significant effects on the dependent variable, as indicated by their low p-values (less than 0.05). Specifically, increasing AGE, CONV, CYBER, EDU, EXPR, and TRUST is associated with an increase in the dependent variable SA. The constant term (C) also has a statistically significant effect on SA.

Table 2. Regression results

Dependent Variable: SA
Method: Least Squares
Sample: 1 477
Included observations: 477

Variable	Coefficient	Std. Error	t-Statistic	Prob.
AGE	0.500953	0.009170	54.62696	0.0000
CONV	1.186468	0.284857	4.165138	0.0000
CYBER	0.682131	0.279635	2.439360	0.0151
EDU	0.902166	0.283975	3.176920	0.0016
EXPR	0.960303	0.285578	3.362664	0.0008
PERSONAL	0.572211	0.286627	1.996359	0.0465
TRUST	1.181892	0.275983	4.282483	0.0000
C	3.205141	0.494267	6.484632	0.0000

R-squared	0.865446	Mean dependent var	23.44070
Adjusted R-squared	0.863437	S.D. dependent var	4.695273
S.E. of regression	1.735109	Akaike info criterion	3.956647
Sum squared resid	1411.974	Schwarz criterion	4.026543
Log likelihood	-935.6604	Hannan-Quinn criter.	3.984129
F-statistic	430.9400	Durbin-Watson stat	2.146412
Prob(F-statistic)	0.000000		

The second part of the table 2 provides additional statistics that help to evaluate the overall performance of the multiple regression model. The R-squared value of 0.865446 indicates that the independent variables explain about 86.5% of the variation in the dependent variable. This means that the model is a good fit for the data and that a large portion of the variability in SA is accounted for by the independent variables. The adjusted R-squared value of 0.863437 is a modified version of R-squared that adjusts for the number of independent variables in the model. It penalizes the inclusion of irrelevant variables in the model and helps to avoid overfitting. The mean dependent variable of 23.44070 indicates the average value of SA in the sample, while the standard deviation of 4.695273 represents the variation around the mean. The standard error of regression (S.E.) of 1.735109 is an estimate of the average distance that the observed data points fall from the regression

line. This measures the overall accuracy of the model in predicting the dependent variable.

The Akaike Information Criterion (AIC) of 3.956647 and the Schwarz Criterion (SC) of 4.026543 are measures of model selection. Lower values of AIC and SC indicate a better model fit. The sum of squared residuals (SSR) of 1411.974 measures the difference between the predicted and actual values of the dependent variable. The F-statistic of 430.9400 tests the overall significance of the model by comparing the variance explained by the regression model to the unexplained variance. A low p-value (less than 0.05) for the F-statistic indicates that the model as a whole is statistically significant. The Durbin-Watson statistic of 2.146412 tests for the presence of autocorrelation in the residuals. A value between 1 and 2 suggests that there is no significant autocorrelation in the model residuals.

Table 3. confidence intervals

Coefficient Confidence Intervals
Sample: 1 477
Included observations: 477

		95% CI		99% CI	
Variable	Coefficient	Low	High	Low	High
AGE	0.500953	0.482933	0.518973	0.477235	0.524671
CONV	1.186468	0.626714	1.746222	0.449728	1.923208
CYBER	0.682131	0.132638	1.231624	-0.041104	1.405367
EDU	0.902166	0.344145	1.460187	0.167707	1.636626
EXPR	0.960303	0.399132	1.521473	0.221697	1.698908
PERSONAL	0.572211	0.008978	1.135444	-0.169108	1.313531
TRUST	1.181892	0.639576	1.724208	0.468103	1.895681
C	3.205141	2.233888	4.176393	1.926791	4.483490

The provided data presents the coefficient confidence intervals of various variables, including AGE, CONV, CYBER, EDU, EXPR, PERSONAL, TRUST, and C. The sample size for this analysis is 477, and all 477 observations are included. The confidence intervals are provided for both the 95% and 99% confidence levels. For the variable AGE, the coefficient is 0.500953, and the 95% confidence interval ranges from 0.482933 to 0.518973, while the 99% confidence interval ranges from 0.477235 to 0.524671. For the variable CONV, the coefficient is 1.186468, and the 95% confidence interval ranges from 0.626714 to 1.746222, while the 99% confidence interval ranges from 0.449728 to 1.923208. For the variable CYBER, the coefficient is 0.682131, and the 95% confidence interval ranges from 0.132638 to 1.231624, while the 99% confidence interval ranges from -0.041104 to 1.405367. For the variable EDU, the coefficient is 0.902166, and the 95% confidence interval ranges from 0.344145 to 1.460187, while the 99% confidence interval ranges from 0.167707 to 1.636626. For the variable EXPR, the coefficient is 0.960303, and the 95% confidence interval ranges from 0.399132 to 1.521473, while the 99% confidence interval ranges from 0.221697 to 1.698908. For the variable PERSONAL, the coefficient is 0.572211, and the 95% confidence interval ranges from 0.008978 to 1.135444, while the 99% confidence interval ranges from -0.169108 to 1.313531. For the variable TRUST, the coefficient is 1.181892, and the

95% confidence interval ranges from 0.639576 to 1.724208, while the 99% confidence interval ranges from 0.468103 to 1.895681. Finally, for the variable C, the coefficient is 3.205141, and the 95% confidence interval ranges from 2.233888 to 4.176393, while the 99% confidence interval ranges from 1.926791 to 4.483490.

Conclusion

Cybersecurity involves a combination of technical, administrative, and physical controls to protect systems and data from cyber threats. Technical controls include the use of firewalls, antivirus software, encryption, and intrusion detection and prevention systems. Administrative controls include policies, procedures, and training to educate employees on the importance of cybersecurity and the proper handling of sensitive information. Physical controls involve securing physical access to systems and devices to prevent unauthorized access.

Cybersecurity also involves the use of risk management frameworks to identify and prioritize cyber risks and implement appropriate controls. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a widely adopted framework that provides guidelines for managing cybersecurity risk. The framework includes five core functions: identify, protect, detect, respond, and recover, which organizations can use to develop their cybersecurity programs.

Cybersecurity is not just the responsibility of organizations; individuals also have a role to play in protecting themselves from cyber threats. Individuals can take several measures to enhance their cybersecurity, such as using strong passwords, enabling two-factor authentication, and avoiding suspicious emails or websites. It is also essential to keep software and devices up-to-date to protect against known vulnerabilities and to regularly backup important data to minimize the impact of a potential cyber-attack.

Governments around the world have also recognized the critical importance of cybersecurity and have implemented various initiatives to promote cybersecurity awareness and best practices. In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) was established to lead the country's efforts to defend against cyber threats. The agency works with public and private sector organizations to share information and coordinate responses to cyber incidents.

International cooperation is also critical in combating cyber threats, given the global nature of the internet and the interconnectedness of systems and networks. The United Nations has established several initiatives to promote international cooperation on cybersecurity, such as the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). The UN GGE provides recommendations and guidelines for promoting responsible behavior in cyberspace and preventing cyber conflict.

To enhance their cybersecurity, banks can take various measures such as implementing a comprehensive cybersecurity strategy, leveraging technology solutions, educating employees and customers, and collaborating with other organizations. One of the essential measures that banks can take is to develop a comprehensive cybersecurity strategy that addresses the specific risks and challenges they face. The strategy should include a risk assessment, a governance framework, security policies and procedures, and incident response plans. The

strategy should be regularly reviewed and updated to address emerging threats and changing regulations. Leveraging technology solutions is also critical for enhancing cybersecurity in the banking industry. Banks can use a range of technologies to protect their systems and data, such as firewalls, intrusion detection and prevention systems, endpoint security solutions, and encryption. Banks can also use machine learning and artificial intelligence to identify and respond to potential threats proactively. Educating employees and customers is another critical measure for enhancing cybersecurity in the banking industry. Banks should provide regular

training to their employees to raise awareness of cyber threats and educate them on best practices for cybersecurity. Banks can also provide educational resources to customers, such as tips for creating secure passwords and avoiding phishing scams.

Collaboration with other organizations is another critical measure for enhancing cybersecurity in the banking industry. Banks can partner with other banks, government agencies, and industry associations to share threat intelligence and best practices for cybersecurity. Collaboration can help banks stay ahead of emerging threats and ensure that they are using the latest cybersecurity technologies and strategies. Moreover, banks can also work with cybersecurity experts to assess their systems and identify vulnerabilities. Penetration testing, vulnerability assessments, and security audits can help banks identify and address weaknesses in their systems and processes.

To enhance their security awareness, online banking customers can take various measures such as using strong passwords, enabling multi-factor authentication, keeping their devices up to date with security patches, and being vigilant about phishing scams.

Using strong passwords is one of the essential measures that online banking customers can take to enhance their security awareness. Passwords should be unique, complex, and not easily guessable. Online banking customers should avoid using common passwords, such as "password" or "123456," and instead use a combination of letters, numbers, and special characters.

Enabling multi-factor authentication is another critical measure that online banking customers can take to enhance their security awareness. Multi-factor authentication adds an additional layer of security by requiring customers to provide a second form of authentication, such as a fingerprint or a one-time code sent to their phone, in addition to their password.

Keeping their devices up to date with security patches is another essential measure that online banking customers can take to enhance their security awareness. Devices that are not up to date with the latest security patches are more vulnerable to cyber threats, such as malware and viruses. Online banking customers should regularly check for software updates and install them promptly.

Being vigilant about phishing scams is another critical measure that online banking customers can take to enhance their security awareness. Phishing scams are one of the most prevalent cyber threats targeting online banking customers. These scams involve cybercriminals sending fraudulent emails or text messages that appear to be from a legitimate source, such as a bank or financial institution. The messages typically include a link or attachment that, when clicked, installs malware on the user's device or redirects them to a fake website designed to steal their login

credentials or other sensitive information. To avoid falling victim to phishing scams, online banking customers should be vigilant and skeptical of unsolicited emails or text messages that ask for personal or financial information. They should also avoid clicking on links or downloading attachments from unknown sources and verify the authenticity of messages by contacting their bank or financial institution directly.

Security awareness of online banking customers is critical in today's digital age. With the increasing use of digital technologies in banking, such as online banking portals, mobile banking apps, and electronic payments, cyber threats have become more prevalent and sophisticated. Online banking customers face various challenges in enhancing their security awareness, such as the increasing sophistication of cyber threats, the need to balance security with convenience, and the lack of awareness of cybersecurity best practices. However, by taking measures such as using strong passwords, enabling multi-factor authentication, keeping their devices up to date with security patches, and being vigilant about phishing scams, online banking customers can enhance their security awareness and protect their accounts and personal information against cyber threats.

References

[1] Z. Gao and N. Ansari, "Tracing cyber attacks from the practical perspective," *IEEE Commun. Mag.*, vol. 43, no. 5, pp. 123–131, May 2005.
[2] W. C. Ashmore, "Impact of alleged Russian cyber attacks," 2009.
[3] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, "Computing the impact of cyber attacks on complex missions," in *2011 IEEE International Systems Conference*, 2011, pp. 46–51.
[4] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification," *Int. J. Secur. Netw.*, 2013.
[5] A. A. Mughal, "Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 2, no. 1, pp. 1–31, 2019.
[6] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technol. Soc. Mag.*, vol. 30, no. 1, pp. 28–38, Spring 2011.
[7] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.
[8] C. Bronk and E. Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* , vol. 55, no. 2, pp. 81–96, May 2013.
[9] J. Raiyn and Others, "A survey of cyber attack detection strategies," *International Journal of Security and Its Applications*, vol. 8, no. 1, pp. 247–256, 2014.
[10] R. Walters, "Cyber attacks on U.s. companies since November 2014," 2015.
[11] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.
[12] A. A. Mughal, "Cyber Attacks on OSI Layers: Understanding the Threat Landscape," *Journal of Humanities and Applied Science Research*, vol. 3, no. 1, pp. 1–18, 2020.
[13] Y. Hideshima and H. Koike, "STARMINE: A visualization system for cyber attacks," in *Proceedings of the 2006 Asia-Pacific Symposium on Information Visualisation-Volume 60*, 2006, pp. 131–138.

[14] A. Bendovschi, "Cyber-attacks–trends, patterns and security countermeasures," *Procedia Economics and Finance*, 2015.
[15] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: A Cyber Attack Taxonomy," 2009.
[16] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," *Congressional research service documents, CRS RL32331 (Washington DC)*, vol. 2, 2004.
[17] O. A. Hathaway *et al.*, "The Law of Cyber-Attack," *Calif. Law Rev.*, vol. 100, no. 4, pp. 817–885, 2012.
[18] A. A. Mughal, "Building and Securing the Modern Security Operations Center (SOC)," *International Journal of Business Intelligence and Big Data Analytics*, vol. 5, no. 1, pp. 1–15, 2022.
[19] K. Huang, M. Siegel, and S. Madnick, "Systematically Understanding the Cyber Attack Business: A Survey," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, Jul. 2018.
[20] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-Attack Modeling Analysis Techniques: An Overview," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 2016, pp. 69–76.
[21] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *J Cyber Secur*, vol. 4, no. 1, p. tyy006, Oct. 2018.
[22] Johnson, "Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation," *NC Banking Inst.*, 2016.
[23] A. A. Mughal, "Cybersecurity Architecture for the Cloud: Protecting Network in a Virtual Environment," *International Journal of Intelligent Automation and Computing*, vol. 4, no. 1, pp. 35–48, 2021.
[24] J. Kosseff, "New York's Financial Cybersecurity Regulation: Tough, Fair, and a National Model," *Geo. L. Tech. Rev.*, 2016.
[25] J. Germano, "Cybersecurity Partnerships," 2014.
[26] T. Poppensieker and R. Riemenschnitter, "A new posture for cybersecurity in a networked world," *McKinsey. March*, 2018.
[27] D. W. Opderbeck, "Cybersecurity, data breaches, and the economic loss doctrine in the payment card industry," *MD Law Rev.*, 2015.
[28] T. Moore, "The economics of cybersecurity: Principles and policy options," *Int. J. Crit. Infrastruct. Prot.*, vol. 3, no. 3, pp. 103–117, Dec. 2010.
[29] A. A. Mughal, "The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection," *International Journal of Intelligent Automation and Computing*, vol. 1, no. 1, pp. 1–20, 2018.
[30] M. A. Terlizzi, F. de S. Meirelles, and M. A. Viegas Cortez da Cunha, "Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance," *Journal of Applied Security Research*, vol. 12, no. 2, pp. 224–252, Apr. 2017.
[31] M. Camillo, "Cybersecurity: Risks and management of risks for global banks and financial institutions," *Journal of Risk Management in Financial Institutions*, vol. 10, no. 2, pp. 196–200, 2017.
[32] D. Grau and C. Kennedy, "Tim lecture series–the business of cybersecurity," *Technology Innovation Management Review*, 2014.
[33] D. Mohammed, "Cybersecurity compliance in the financial sector," *The Journal of Internet Banking and Commerce*, vol. 20, no. 1, pp. 1–11, 1970.
[34] M. Rizal and Y. Yani, "Cybersecurity policy and its implementation in Indonesia," *J. ASEAN Stud.*, vol. 4, no. 1, p. 61, Aug. 2016.

[35] B. Fonseca and J. D. Rosen, "Cybersecurity in the US: Major Trends and Challenges," in *The New US Security Agenda: Trends and Emerging Threats*, B. Fonseca and J. D. Rosen, Eds. Cham: Springer International Publishing, 2017, pp. 87–106.
[36] A. A. Mughal, "Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions," *Journal of Artificial Intelligence and Machine*, 2018.
[37] A. W. Ng and K. B. K. B., "Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator," *Journal of Financial Regulation and Compliance*, vol. 25, no. 4, pp. 422–434, Jan. 2017.
[38] R. Zhu, "An initial study of customer internet banking security awareness and behaviour in China," 2015.
[39] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Comput. Secur.*, vol. 68, pp. 145–159, Jul. 2017.
[40] A. A. Mughal, "Well-Architected Wireless Network Security," *Journal of Humanities and Applied Science*, 2022.
[41] F. A. Aloul, "The need for effective information security awareness," *Journal of advances in information technology*, 2012.