Journal of Posthumanism
2025
Volume: 5, No: 8, pp. 461–468
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i8.3205

The Relationship between Cyber Immunization, Cyber Resilience, Cyber Threat, and Fear of Cybercrime

Jassim Abdulla Alkhater[1], Diab M. Al-Badayneh[2]

Abstract

This study investigates the interrelationship between cyber immunization, cyber resilience, cyber threat exposure, and fear of cybercrime. In particular, it explores how variations in cyber knowledge and experiences of cyber victimization influence these constructs. The study used a social survey. A special questionnaire was developed with a high reliability coefficient (Cronbach's alpha 0.946). Data was collected using a questionnaire from a convenient sample of (190) individuals from the Qatari Ministry of Interior. The tool demonstrates strong face and construct validity, as evidenced by the relationship between cyber threats and fear of crime ($r = 0.369$, $\alpha = 0.00$). The study found that citizens have a high awareness of some of the most significant cyber threats; over 60 percent recognize major internet security breaches occurred recently (63.2 percent), and more than half know about large data losses (60.5 percent). Cybersecurity threat, immunity and resilience, and knowledge together explain 20.0% of the variance in fear of cybercrime (p = <.001). Further, the study highlights the combined response of cognitive and emotional factors in perceiving cyber risks. When fear of cybercrime increases, and when a provider knows an individual that commits an IT crime, these factors would contribute to enhancing immunity against electronic threats. In terms of cybercrime, knowledge and resilience are efficient types of capable guardianship, which result in less stress affecting the mind. To offer a solution, organizations (primarily those involved in security and national infrastructure) should focus on fostering cyber immunization strategies, resilience training, and continual awareness programs.

Keywords: *Cyber Opportunity, Cyber Resilience, Cyber Victimization, Cyber Perpetrators, Low Self-Control, Cybercrime, Qatar.*

Introduction

Cybercrime has thus become an increasing concern to individuals and organizations due to rapid advancements in the digital world. In a world where technological usage increases daily, so, too, do the threats it poses to societies. The digitalization world has transformed rapidly, and with it brought new challenges for individuals and organizations. (Yar, 2013; Wall, 2007). Societies are becoming ever more reliant on digital technologies, and with this, new fears of potential victimization have struck. (Lee & Gibbs, 2015). Various studies and literature have supported the need to understand the psychological and behavioral reactions to cybersecurity threats. It will be effective by exposing certain vital concepts that could reduce fears caused by cybercrime. They include cyber immunization, which refers to proactive behaviors and preparedness against online threats, and cyber resilience, referring to an individual's ability to recover from such threats. Simultaneously, the past decade has recorded enhanced fears regarding the exposure to

[1] Department of Security Studies, Graduate College, Police Academy, MOI, Email: Jassimalkhater@gmail.com, 0009-0004-8616-626X

[2] Ph.D. Methodology, Criminology, and Security Studies, Department of Security Studies, Graduate College, Police Academy, MOI, Qatar & IKCRS, Amman, Jordan, Email: dbadayneh@gmail.com, (Corresponding Author), ORCID 0000-0001-7416-6722

vulnerability within cyberspace. The rapid growth of digital technologies has significantly altered criminal behavior, sparking new forms of cybercrime. Ecological and psychological components define the extent to which a person victimizes or is victimized by cybercrime. Some major constructs include cyber opportunity, cyber resilience, cyber victimization, cyber perpetration, and low self-control. (Bossler & Holt, 2009). Cyber resilience entails individuals' increasing dependency on digital technologies for communication, work, and daily routines. It plays a major role in broadening the number of victims and offenders. With increased digital engagement comes high exposure to cyber risks, such as fraud, cyberbullying, and phishing. Moreover, these activities increase the likelihood of normalization of deviant behaviors like digital piracy and trolling. (Holt & Bossler, 2014). Cybercrime is the use of digital technology to commit and/or facilitate a crime; it takes many forms, including phishing (the practice of using email messages that appear to be from legitimate organizations but are actually malicious), identity theft, distribution of malware, and unauthorized access or third-party monitoring. and denial-of-service attacks (Wall, 2007; Al-Badayneh, 2024). This trend represents a major risk to individuals, businesses, and nations in general and the world economy overall. Cybercrime is often veiled and therefore underreported or sometimes even overlooked. Therefore, combating it requires the deployment of sophisticated information technologies and internationally coordinated policies. A common element that defines cybercrime is the compromise of information, data, or systems. To respond to these consequences effectively, flexible and timely interventions are needed (Clough 2015).

Al-Badayneh et al.'s (2024a, 2024b) study explored victimization, perpetration, and awareness of the Qatari Cybersecurity Law (QCL) among 209 Qatari students from three universities. The study found that 23% of students reported being victims of cybercrime, while 6% admitted to engaging in cybercrime. Although general understanding of the QCL was below average, a large proportion of students were aware of its existence, recognized punishable crimes, and could cite illicit behaviors. The study revealed significant differences in levels of victimization, perpetration, and awareness of the QCL.

Cybercrime in Qatar involves online fraud, identity theft, malware, phishing, cyberbullying, and cyber blackmailing. To report a cybercrime, users must use the Metrash2 app and send a complaint photo. The Qatari government introduced a cybercrime prevention law in 2014, imposing sanctions and penalties. Critics argue it threatens freedom of speech and media access. The New Protection of Personal Data Privacy Law in 2017 imposes obligations on individuals and entities collecting and processing personal data. Qatar's National Cyber Security Agency (NCSA) has introduced a National Incident Management Framework to tackle rising cyber threats, including espionage, financial data breaches, and infrastructure outages. The framework focuses on command, control, detection, investigation, strategic response, system recovery, regulation, standards, compliance, and incident review.

Methodology

Sample

The study used the social survey method, and data were collected using an e-questionnaire from a sample of 190 employees of the Ministry of Interior, of whom 78.9% were male and 21.1% were female.

Measurement

The questionnaire was developed as a data collection tool. The questionnaire was composed of eight sections, as follows:

Part One: Demographic Data. This included gender, educational qualifications, age, and years of experience. This section also included questions about the number of hours spent online per day, knowledge of cybersecurity, internet security vulnerabilities, cyberattacks on state infrastructure, hacking of citizens' data, cyber breaches of personal social media accounts, and financial cyber fraud.

Part Two: Cyber Threats. This section included (10) questions related to the most prominent cybersecurity threats from the study sample's perspective.

Part Three: Cybersecurity Immunization. This section included (10) questions related to the most prominent cybersecurity safeguards from the study sample's perspective.

Part Four: Cybercrime. This section included six) questions related to the nature of cybercrime and its consequences from the study sample's perspective.

Part Five: Cyber Resilience. This part included (6) questions related to cyber resilience among the study sample.

Part Six: Knowledge. This part included (6) questions related to knowledge of the Qatari Anti-Cybercrime Law of 2014.

Part Seven: Perpetrators. This part included (6) questions related to the likelihood of committing a cybercrime among the study sample.

Part Eight: Victims. This part included six) questions related to the likelihood of an individual falling victim to a cybercrime among the study sample.

The questionnaire's sections were graded according to the five-point Curt scale (1-strongly agree, 2-agree, 3-neutral, 4-disagree, 5-strongly disagree), the four-point scale (1-don't know, 2-simple knowledge, 3-good knowledge, 4-extensive knowledge), and the two-point scale (1-yes, 2-no).

Validity

To ensure the validity of the instrument, it was presented to five) reviewers who are e specialists the topic. 95% consensus of all items was accomplished.

Construct Validity. To enhance the validity of the instrument, the construct validity of the study instrument was verified, using the relationship between cyber threats and fear of crime ($r = 0.369$, $\alpha = 0.00$).

Reliability

The instrument's reliability was assessed using Cronbach's alpha. The reliability coefficient for cybersecurity threats was 0.946; cybersecurity immunization, 0.974; cybercrime, 0.890; cyber resilience, 0.732; knowledge, 0.749; perpetrators, 0.808; and victims, 0.882.

Findings

Table 1 shows that more than half of the sample had knowledge of security breaches and attacks on citizens' data, and about a third of them had heard about cyberattacks. Moreover, around a quarter of the sample experienced cyberattacks or cyber financial losses.

Item	Yes %
In the last 6 months, have you **heard about any security breaches** on the internet?	63.2
have you **heard about a cyberattack** on the country's infrastructure?	30.5
have you **heard about a hack** of citizens' data?	60.5
have you **experienced a cyberattack** on your personal social media accounts?	21.6
have you **experienced a cyberattack that resulted in financial losses**?	17.9

Table 1 Percent of Yes Answers for Knowledge Questions

Table 2 shows results of testing the relationships, suggesting that cyber threats are strongly related to cyber immunization, fear of cybercrime, and cyber offenders. There are also relationships between cyber immunization and fear of crime, as well as between the offenders and victims themselves. The relationships between fear for cybercrime and cybercrime itself, between perpetrators and victims of cybercrimes, and among resilience, vulnerabilities, and knowledge are also found to be significant. Moreover, the experiences that victims of cybercrime have with their personal traits and knowledge are associated both positively with cyber resilience and negatively with knowledge.

	Cyber threats	Cyber immunization	Fear of Cybercrime	Cyber perpetrator	Cyber victim	Cyber resilience	knowledge
Cyber threats	1						
Cyber immunization	.761**	1					
Fear of Cybercrimes	.369**	.447**	1				
Cyber perpetrator	-.223**	-.280**	-.146*	1			
Cyber victims	-.065	-.145*	-.044	.812**	1		
Cyber Resilience	.134	.133	.094	.159*	.231**	1	
knowledge	.000	.024	.051	.418**	.424**	.197**	1

Table 2: The Relationship between Cyber Threats, Cyber Immunization, Fear of Cybercrimes, Cyber Perpetrators, Cyber Victims, Cyber Resilience, & Cybercrime

α ** .001 * .05

Table 3 presents significant effects of cyber perpetrators, experience, internet use, cyber penetration, security breaches, cyber threats, resilience, knowledge of cybersecurity, cyber-attacks, personal hacking, cyber fraud, and immunization of victims on fear of cybercrimes

(F=3.866, α=.00). All these variables explained 26% of the variance in the fear of cybercrimes.

	Source	Sum of Squares	df	Mean Squares	F	α
Fear of cybercrime	Regression	147.928	13	11.379	3.866	.000
	Residual	415.014	141	2.943		
	Total	562.942	154			

Table 3

Regression ANOVA table of the effects of cyber perpetrators, experience, internet use, cyber penetration, security breaches, cyber threats, resilience, knowledge of cybersecurity, cyber-attacks, personal hacking, cyber fraud, and immunization of victims on fear of cybercrimes.

Conclusion

The research revealed that citizens know about major cyber threats and issues, with 63.2% hearing about the recent internet security breaches and 60.5% aware of how breaches are causing concern around citizens' data. More than 30.5% are aware of cyber attacks on national infrastructure as well. 21.6% suffered attacks targeting their social media accounts, landing 17.9% in the red as a result; and higher cyber immunization is significantly and positively correlated with more knowledge about cybersecurity threats—underscoring the crucial role that these efforts perform in cybersecurity risk consciousness and comprehension. Furthermore, heightened fear of cybercrime is related to increased detection of cyber threats, and when people perceive themselves at risk, they may not trust a diverse set of strategies for ensuring cybersecurity.

Testing the corresponding hypotheses reveals that cyber threats are very important when it comes to cyber immunization, fear of cybercrime, and finding out if a provider knows someone who has committed an IT crime is statistically significant. There are also correlations between cyber immunization and fear of crime (offenders and victims). There are significant relationships regarding fear of cybercrime, as well as the dynamics between offenders and victims and the interplay among resilience, vulnerabilities, and knowledge. The outcomes suggest that the experiences of cybercrime victims, coupled with personal characteristics and knowledge, are associated both positively with cyber resilience and negatively with knowledge. Together, these findings illustrate the interplay of psychological and behavioral factors within current cyber threat landscapes, which is why it is vital to pursue elevated levels of cyber immunization, resilience, and knowledge as countervailing responses against the damaging impacts or consequences of potential malicious incursions.

Altogether, while the results of this analysis suggest widespread worry about cyber threats, there are still many worries and fears on a large scale. Because of this we will require more advanced cyberspace immunization defense as well as educational campaigns to counter the relative ease with which militaries (Rosenthal & Martin, 2020) can use RO status for military advantage. Addressing these fears requires better cybersecurity and more awareness among the public, which will ultimately make the country more resilient against cyber incidents.

Discussion

This study explores the problem of cyber immunization in addition to knowledge, cyber resilience, cyber threats, and the fear of cybercrime while also considering varying degrees of cyber victimization. It is the recent research that focuses on the psychological and behavioral reactions to the threats in cybersecurity. Cyber immunization, which can be considered how one is proactive and ready for the online threats, and cyber resilience, or the ability to withstand possible cyber incidents and recover, are identified as playing an alleviating role in cyber fear. At the same time, the increasing feeling of being under threat of cyberspace intrusion remains a strong indicator of the fear. Analysis shows that cyber vulnerability and cyber threats correlate with fear from cybercrime ($r = 0.369$ and $r = 0.447$, $p < 0.001$). In addition, multiple regression analysis shows a joint meaningful effect of cyber threats and cyber vulnerability, immunization and resilience, and learning to fear cybercrime. Therefore, fear in the digital world is multidimensional, requiring education and boosting citizens' insights to eliminate the psychological impacts. These findings highlight the multifaceted nature of fear in the digital environment and underscore the importance of enhancing cyber literacy and resilience to address psychological impacts of cyber threats. These findings are consistent with prior research indicating that perceptions of online risk and personal vulnerability contribute significantly to the formation of cyber-related anxieties (Bossler & Holt, 2012; Räsänen et al., 2016).

The multiple regression analysis, which found that cybersecurity threats, immunization, resilience, and knowledge collectively explain 20% of the variance in fear of cybercrime ($F = 9.449$, $p < 0.001$; $R^2 = 0.20$), highlights the interplay between cognitive and emotional factors in cyber-risk perception. This supports prior literature emphasizing the need for both technological preparedness and psychological resilience to mitigate fear responses in cyberspace (Ngo & Jaishankar, 2017; Wendt, 2020). As previous research suggests, individuals who possess higher levels of cyber literacy and psychological readiness are better equipped to manage digital risks and thus experience lower levels of fear (Marcum et al., 2014; Hadlington, 2017).

These findings also align with criminological theories such as the Routine Activity Theory and Fear of Crime Framework, which posit that individuals' perceptions of vulnerability, guardianship, and risk significantly shape their fear experiences (Yar, 2005; Ferraro, 1995; Wilcox, 2015; Williams, 2016).). In the context of cybercrime, knowledge and resilience function as forms of "capable guardianship" that help reduce psychological distress.

Overall, this study underscores the urgent need for organizations—especially those involved in security and national infrastructure, such as the Ministry of Interior—to promote cyber immunization strategies, resilience training, and continuous cyber awareness programs. Enhancing individuals' capacity to detect, respond to, and recover from cyber threats can meaningfully reduce the psychological burden associated with digital exposure.

References

Al-Badayneh, et al. (2024). Cyberbullying, Victimization, Strains And Delinquency In Qatar. European Journal of Science and Theology 18(6):65-76

Al-badayneh, D. M. (2014). Cybercrimes: Definition and causes: Research paper for the Conference on New Crimes in Light of Regional and International Changes and Transformations, College of Strategic Sciences, Amman, Jordan.

Al-Badayneh, D., Al Dosari H., Al Qahtani, H., Alkhater, J., & Mehawesh, S., (2024a). College Students Attributional Differences in Knowledge Awareness About a Cybercrimes Law. Journal of Ecohumanism. Volume: 3, No: 6, pp. 773 – 786 ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online) https://ecohumanism.co.uk/joe/ecohumanism DOI: https://doi.org/10.62754/joe.v3i6.4046. https://ecohumanism.co.uk/joe/ecohumanism/article/download/4046/3299/12050

Al-Badayneh, D., Mehawesh, S., Alkhater, J., Al Qahtani, H., ,& Al Dosari, H. (2024b). The Relationship between Knowledge Awareness about Qatari Cybersecurity Law, Victimization, and Perpetration Experience: Some Applications of Routine Activities Theory. Contemporary Readings in Law and Social Justice. ISSN: 1948-9137, e-ISSN: 2162-2752. Vol 16 (1), 2024 pp. 1115 – 1128

Bossler, A. M., & Holt, T. J. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1–25. https://doi.org/10.1080/01639620701775438

Bossler, A. M., & Holt, T. J. (2012). The effect of self-control on victimization in the cyberworld. Journal of Criminal Justice, 40(5), 417–424.

Ferraro, K. F. (1995). Fear of Crime: Interpreting Victimization Risk. SUNY Press.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346.

Holt, T. J., & Bossler, A. M. (2014). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. American Journal of Criminal Justice, 37(3), 378–395.

Lee, J., & Gibbs, J. P. (2015). Fear of crime in cyberspace: Examining the impact of perceived cyber threats, previous victimization, and risk perceptions on fear of cybercrime. International Journal of Cyber Criminology, 9(1), 1–20.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Freiburger, T. L. (2014). Exploring the effects of parental controls on cyberbullying victimization in a youth sample. Youth & Society, 46(3), 446–464.

Ngo, F. T., & Jaishankar, K. (2017). Cyber routine activities theory: A theoretical framework for understanding cybercrime victimization. In Holt, T. J. (Ed.), Cybercrime Through an Interdisciplinary Lens (pp. 231–245). Routledge.

Phillips, K., et al. (2020). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sci. 2022, 2(2), 379 398; https://doi.org/10.3390/forensicsci2020028. https://www.mdpi.com/2673-6756/2/2/28

Räsänen, P., Hawdon, J., Holkeri, E., Keipi, T., & Oksanen, A. (2016). Targets of online hate: Examining determinants of victimization among young Finnish Facebook users. Violence and Victims, 31(5), 711–729.

Rosenthal, R., & Martin, D. (2020). Cybersecurity awareness: A vital component in preventing cybercrime. Journal of Cybersecurity Studies, 15(3), 45-59.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity.

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity.

Warren S. & Maakaron, C., (ND). Qatar's New Protection of Personal Data Privacy Law. Squire Patton Boggs.

Wendt, M. (2020). Cyber resilience and the human factor: Operationalizing cybersecurity culture for organizations. Journal of Strategic Security, 13(1), 1–18.

Wilcox, P., (2015). Routine Activities, Criminal Opportunities, Crime and Crime Prevention, Editor(s): James D. Wright, International Encyclopedia of the Social & Behavioral Sciences (Second Edition), Elsevier, Pages 772-779, ISBN 9780080970875, https://doi.org/10.1016/B978-0-08-097086-8.45080-4. (https://www.sciencedirect.com/science/article/pii/B9780080970868450804)

Williams M.L., (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level, The British Journal of Criminology, Volume 56, Issue 1, Pages 21–48, https://doi.org/10.1093/bjc/azv011 https://academic.oup.com/bjc/article/56/1/21/2462277

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. European

Journal of Criminology, 2(4), 407–427. https://doi.org/10.1177/147737080556056

Yar, M. (2013). Cybercrime and society. SAGE Publications.