Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 16 (1), 2024
pp. 1115 - 1128

The Relationship between Knowledge Awareness about Qatari Cybersecurity Law, Victimization, and Perpetration Experience: Some Applications of Routine Activities Theory

Diab M. Al-Badayneh[1] Sada S. Mehawesh[2],Jassem A. Alkhater[2],Hamed M. Al Qahtani[2],& Hamad M. Al Dosari[2]

1 Ph.D. Methodology, Criminology, and Security Studies

dbadayneh@gmail.com

ORCID 0000-0001-7416-6722

Department of Security Studies, Graduate College, Police Academy, MOI, Qatar &IKCRS, Amman, Jordan

[2]ssajm1986@gmail.com

0009-0007-8095-9287

[2]Jassimalkhater@gmail.com

0009-0004-8616-626X

[2]hmf_5060@hotmail.com

0000-0003-3533-6922

[2]hmh458@outlook.com

0009-0007-2125-0323

[2]Department of Security Studies, Graduate College, Police Academy, MOI

Abstract: The study examines the relationship between knowledge awareness about Qatari cybersecurity law (QCL), victimization, and perpetration experience. The study describes and tests the differences in exposure to perpetration and victimization in terms of victimization and perpetration experience, knowledge about QCL, and attitudes towards QCL. The study sample consisted of 209 Qatari students, representing three Qatari universities. Of these, 163 (78%) were males, and 46 (22%) were females. Students (23%) reported being victims of cybercrimes, and 6% were perpetrators. The students spent an average of 4 hours on the internet, with a standard deviation of 5.3. The study used a survey as a research instrument. The questionnaire included knowledge about the QCL scale (9 items with reliability Cronbach's alpha =.79), perpetration experience (8 items with reliability Cronbach's alpha =.86), victimization experience (8 items with reliability Cronbach's alpha =.83), and an attitude scale (29 items with reliability Cronbach's alpha =.96). All scales are based on a literature review. We categorized all scales into interval levels 0–5, with 0 to 5 being the most frequently used. The findings showed that students' knowledge of GCL was below average, with the highest percentage of students learning about the QCL (66.5%), hearing about a cybercrime conviction (56%), and witnessing behaviors in cyberspace that required punishment (48.8%). 8.8%). Students experienced online banking fraud as the most common crime, accounting for 28%, followed by denial of service (DOS) at 17% and identity theft at 15%. A small percent of students reported committing cybercrimes, mostly digital piracy (15%) and online banking fraud (10.5%). Significant differences attributed to perpetration exposure (yes-no answer) were found in victimization experience (F = 26.470, α =.000), perpetration experience (F = 40.082, α =.000), and knowledge about QCL

(F = 7.451, α =.007). Finally, ANOVA results showed that perpetrator experience (F = 13.355, ± =.000), victimization experience (F = 28.032, ± =.000), and knowledge about QCL (F = 7.804, ± =.006) were all different when the answer was "yes" or "no.". We discussed some applications of Routine Activities Theory (RAT).

Keywords. Qatari cybercrimes, Qatar, Victimization, Perpetration, Knowledge.

Received:17 March 2024 **Revised:** 20 May 2024 **Accepted:**18 June 2024

Introduction

Cybercrime poses a significant threat to the global economy, individual states, and businesses, resulting in significant costs and losses. It involves data corruption, theft, intellectual property, and reputation damage. Despite the rapid growth of cybercrime, detection and prosecution are rare. A need for strategies for modernizing information systems should be developed to reduce cybercrime scale and create international policy principles. (Sviatun, Goncharuk, Roman, Kuzmenko, &^ Kozych, 2021). Cybercrime is a growing problem in today's internet-dependent society, targeting individuals through various online activities such as phishing, scams, online harassment, identity theft, malware, hacking, and denial-of-service crimes. Cybercrime can result from weak cyber security, new technologies, and business schemes. It is crucial for businesses to prioritize cybersecurity measures and develop strong defenses against cyberattacks. Despite efforts to slow down attacks, they have not been successful. The paper suggests spreading awareness about cybercrimes and imposing strict punishments on cybercriminals to discourage crime. It also emphasizes the need for appropriate laws and strict enforcement of laws to prevent further cybercrime. Cybercrime can take many forms, including phishing, identity theft, hacking, spreading hate, child pornography, grooming, copyright infringement, selling illegal items, and soliciting child pornography. Some crimes have come to light, while others remain a mystery. To protect against these issues, users install virus protection software and use unique passwords. Internet crimes against children are a concern, and while the internet is an essential part of our lives, it poses serious threats. (Deoral & Chudasama, 2021).

Cybercrime is a transnational crime that involves organized crime groups and affects societies all over the world. It is divided into two categories: technological and human-based. Traditional crimes involve computer viruses, bank account thefts, and fraud using plastic payment cards. Cybercrime can spread to different regions and require an urgent, dynamic response. The proliferation of computer technologies has positively impacted the economy, but it can also disrupt businesses and government agencies. Cybercrime can take the form of traditional crimes, which have a more visible human element, or new crimes involving computer technology. Cybercrime refers to internet-related crimes such as computer virus development, bank account theft, and plastic card fraud. The complexity of detection, investigation, latency, damage, and court cases makes it challenging to prosecute them. (Sviatun, Goncharuk, Roman, Kuzmenko, & Kozych, 2021). Cybercrime is a complex issue that can be difficult to understand. One major issue is the lack of recording mechanisms that accurately distinguish between online and offline crimes. Police recorded crimes do not distinguish between online and offline offenses, making it difficult to identify cyber crimes. The implementation of Action Fraud, a national reporting center for fraud and financially motivated cybercrime, aims to gather reports from the public and businesses, categorize them, and evaluate them based on the Home Office Counting Rule. However, underreporting of cyber crimes persists, and there is a lack of awareness that certain cyber incidents qualify as crimes. y crimes. (McGuire & Dowling, 2013). Cybercrime refers to the destruction, theft, or unauthorized use of information, programs, services, equipment, or communication networks. It is a worldwide problem involving the use of technology like computers, smartphones, or tablets. According to the Council of Europe, it is defined as any criminal offense committed against or with the assistance of a computer network. (Abu Taher & Jahan, 2020). According to Al Anazi (2019), transnational crimes are defined as geographically distant, soft crimes that are difficult to prove, simple to implement, attractive to criminals due to large gains, and difficult to control damage compared to traditional crimes. AlZeben and AlKharabsheh's (2021) study The study recommended that university courses spread awareness of cybercrime risks and target them. AlZeben, G., AlKharabsheh, A. (2021).

Qatari Definition of Cybercrimes Law

Various forms of cybercrime in Qatar include online fraud, identity theft, malware, phishing, cyberbullying, and cyberblackmailing. To report a cybercrime, users must log in to the Metrash2 App, navigate to the "Communicate with Us" section, select the appropriate department, attach a complaint photo, choose the type of complaint, provide location and details in brief, enter their phone number, and click on "Send." This action sends the report to the relevant authorities for further investigation. Staying well-informed and vigilant is critical to protecting oneself and their information from cyber threats. (Team Qatar Talk, 2023).

The Qatari government has introduced a cybercrime prevention law (No. 14 of 2014) to combat online and cyber crimes. The law imposes sanctions and penalties for offenses committed through the internet, IT networks, and computers. It aims to protect the country's technological infrastructure and strengthen cyber security. Critics criticized the law for threatening freedom of speech and media access. The law includes penalties for forging official e-documents, impersonating individuals or entities, identity theft, and stealing property. It also prohibits publishing "false news" and imposing jail terms for unauthorized e-card possession or use. The law also imposes fines for breaching intellectual property rights. Cybercrimes are the second most common form of economic crime in the Middle East, posing a high risk to businesses. (Al Tamimi & Co., 2024). Article 8 of Law on Combating Cyber Crimes (Law No. 14 of 2014) stipulates that a sentence of not more than three years in prison and a fine of not more than QR100,000, or either of these penalties, shall be imposed on any person who, through an information network or information technology technique:

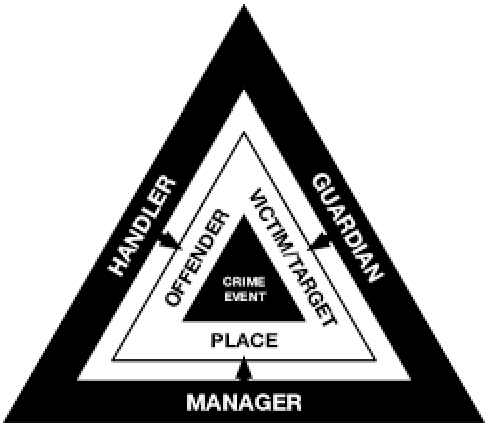
violates social values or principles.

publishes news, photos, video, or audio recordings related to the sanctity of people’s private or family life (even if the same is true) or insults or slanders others. (Regi, 2020).

Qatar’s New Protection of Personal Data Privacy Law. The New Law. On January 29, 2017, Law No. 13 of 2016 on the Protection of Personal Data and Privacy (the "New Law") entered into force. Individuals and entities subject to the New Law were initially required to comply with its provisions by July 29, 2017. However, we understand that the New Law has extended this compliance deadline until January 29, 2018. Any individual or entity collecting and electronically processing personal data. "Personal data" is generally defined as "any information relating to an individual identified or reasonably identifiable by reference to such information or by combining such information with any other information." As a result, the New Law has an impact on employers, healthcare providers, universities, and B2C entities, as well as any entity or individual supporting them in the collection and/or processing of personal data. The law also covers those who supply cloud or other remote data processing services. Failure to follow the New Law can lead to fines of up to QR5 million (US$1.3 million). Any contract or agreement concluded in violation of the New Law, to the extent of its violation, shall be considered null and void. The New Law establishes two categories: "controllers," defined as the entity who "determines the means and purposes of processing personal data," and "processors," defined as the entity who "processes personal data on behalf of a controller." Warren & Maakaron, ND) The law outlines various measures, including forgery penalties, impersonation and theft, content crimes, unauthorized use of e-cards, intellectual property rights, and insult and libel. The rising threat of cybercrime mirrors the challenges faced globally as reliance on digital technologies increases. (Team Qatar Talk, 2023).

Routine Activities Theory

Lawrence Cohen and Marcus Felson developed Routine Activities Theory (RAT) in 1979, focusing on three factors: potential offender, suitable target, and lack of capable guardian. It relies on a rational choice methodology and situational crime prevention techniques. However, it has criticisms, such as assuming criminals are rational, unaware of security measures, or under influence. (Purpura, 2013) It explains how changes in society's routine activities can increase or decrease opportunities for crime.



The 'crime triangle' of routine activity theory. (IFE et. Al., 2019, p. 9)

RAT posits that for a crime to occur, three elements must converge:

A motivated offender: someone ready and willing to commit a crime.

A suitable target: a person, object, or place that is attractive to the offender.

The absence of a capable guardian results in a lack of protection, which could be provided by a person or security measures. RAT emphasizes that crime is situational, meaning that it arises due to opportunities rather than offenders' characteristics. For example, during economic growth, increased material wealth may lead to more thefts, as more valuable targets are available with less supervision (Cohen & Felson, 1979). In the late 20th century, criminology developed a framework focusing on crime as a result of situation-specific opportunity. This framework incorporates routine activity theory and other perspectives on situational opportunity. Today, we integrate these theories to create a broader perspective on crime opportunity. (Wilcox, 2015).

Application of RAT to Cybercrime

In the digital age, cybercrime has grown in complexity and volume, and RAT offers insights into why certain individuals or systems become victims of online attacks. Modern applications have extended RAT to cybercrime. The theory explains that motivated offenders use the anonymity of the internet to find suitable digital targets (e.g., personal data) with limited cybersecurity ("guardianship") (Bossler & Holt, 2009). Here's how each element of RAT applies to the cyber world:

Motivated Offender:

In cybercrime, motivated offenders range from individuals engaging in criminal activities for financial gain (e.g., phishing or identity theft) to nation-states involved in espionage or sabotage. The anonymity provided by the internet lowers the risk of apprehension, making criminal activities more attractive. Research shows that the internet enables a broader pool of motivated offenders, as cybercrimes often require less physical effort and risk compared to traditional crimes (Miro, 2014).

Suitable Target

Digital assets, such as personal information, financial data, or intellectual property, are often the target. The value of these digital assets makes them attractive to cybercriminals. Research has identified that certain behaviors increase vulnerability. For example, individuals who frequently share personal information online or engage in risky digital behaviors (such as using weak passwords) are more likely to become targets (Leukfeldt & Yar, 2016).

Absence of a Capable Guardian:

"Guardians" in cybercrime include anti-virus software, firewalls, encryption, and secure browsing practices. However, the vastness of the internet and the often inadequate cybersecurity measures taken by individuals or organizations lead to opportunities for cybercriminals. A key issue is that many individuals are unaware of basic cybersecurity practices, and small businesses or vulnerable organizations may not invest sufficiently in capable defenses. This lack of cyber guardianship leads to heightened risks (Bossler & Holt, 2009).

LITERATURE REVIEW

Cybercrime: The concept

Cybercrime is a term used interchangeably by various organizations, including the United Nations, the United Nations Office on Drugs and Crime, the Council of Europe Cybercrime Convention, the Commission of European Communities, the European Union's Cybersecurity Strategy, the Commonwealth of Independent States Agreement, the European Union's Directive on Attacks against Information Systems, the Asia-Pacific Economic Cooperation (APEC), Interpol, Thomas and Loader, Gordon and Ford, Europol, the European Cybercrime Center, and the U.S. Department of Justice. The UNODC defines cybercrime as any illegal behavior directed by electronic operations that targets the security of computer systems and data processed by them. Cybercrime, according to the European Cybercrime Center, is any crime that requires the use of computers, computer networks, or other forms of information and communication technology (ICT). The U.S. The Cybercrime Law No. 17 of 2023 criminalizes activities like unauthorized access to information networks, fake accounts, misinformation, phishing, and illegal donations, as well as prohibiting promoting prostitution, obtaining information on weapons, and possessing electronic data. (Al-Badayneh et al., 2024).

Related Literature Review

Cybercrime presents a global threat to national security and disrupts international relations. Experts estimate that cybercrime and cybersecurity will cost over one trillion US dollars by 2020. The study by Sviatun et al. (2021) examines the interrelationship between cybercrime, cybersecurity, and legal counteraction methods in different countries, emphasizing the importance of international cooperation in developing global strategies. (Sviatun, Goncharuk, Roman, Kuzmenko, & Kozych, 2021). AL-badayneh et al. (2024) analyzed the knowledge of Jordanian Cybercrimes Law in four Jordanian universities. The majority of the students were victims of cybercrimes, while 24% were perpetrators. According to the study, females were more knowledgeable about the law than males, and there were significant external attribution differences in knowledge. (AL-badayneh et al., 2024)

Cyberbullying, a form of cybercrime, has become more prevalent in Qatar. The Cybercrime Prevention Law No. 14 of 2014 recognizes cyberbullying in Qatar as the use of online services to bully or harass a person with the intent to harm them socially, psychologically, or even physically. The rise of social media and digital communication has led to an increase in cyberbullying cases, affecting students' mental health and well-being. Platforms that facilitate anonymous interactions have become hotspots for cyberbullying, underscoring the need for improved digital literacy and online safety education (Alrajeh et al., 2021; Dou et al., 2020; Gohal et al., 2023). Alrajeh et al. (2921) conducted a study in Qatar. The study found that most students are involved in cyberbullying, with approximately 50% experiencing depression symptoms. Researchers discovered significant correlations among cyberbullying experiences, gender, depression, and the relationship between cyberbullying and depression. (Alrajeh et al., 2921) Cyberbullying is a common problem among university students worldwide, with a prevalence of 11%–55%. Despite Qatar's 100% internet penetration and criminalizing initiatives, there is a lack of research and awareness on the issue. (Foody et al., 2016) In 2011, the Global School-based Student Health Survey revealed that over 43% of surveyed youth reported experiencing bullying. (Global School-based Student Health Survey, 2018). Qatar has the 19th highest rate of cyberbullying out of 25 countries, with higher rates of online bullying and concerns among students. (Microsoft, 2018).

In the UAE, a study found that university students have a medium level of knowledge about cybercrimes, with 21.5% specializing in computer information technology having the highest knowledge. This is in line with a strong correlation between knowledge and the use of internet technology. The findings suggest that young adults should be more educated about the risks of using technology and develop strategies to raise awareness. (Bamatraf, 2014). The Jordanian Cybercrimes Law does not adequately address the crimes of electronic defamation, libel, and slander, which are the most prevalent cybercrimes in Jordan. The law lacks a comprehensive legal framework, as it only has one article on these crimes. For these crimes, the Jordanian Penal Code and the Jordanian Code of Criminal Procedures provide general rules. The law has taken a tough approach, imposing severe punishments and subjecting the commission to detention and confiscation. To address these issues, public awareness should be raised, statistics on the scale of these crimes should be published, the law should include a provision for personal claims, and a comprehensive legal framework should be established. (Al-Zoubi, 2023).

Cybercrimes involve unauthorized network breaches or theft of intellectual property or data, with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm or loss, using modern telecommunication networks like the internet and mobile phones. Cybercrime threatens security and financial health, with law enforcement typically handling its response. Cyberwarfare involves actions by nation-states or international organizations to attack and damage another nation's computers or information networks, often motivated by greed, power, or emotional and physical harm. It can facilitate conventional attacks or spread propaganda. Cyberterrorism is the deliberate use of disruptive activities against computers and networks to cause harm or further social, ideological, religious, political, or similar objectives. Cyberterrorism differs from other types of cybercrime because it conceals the intent of individuals or groups. Cybercriminals use profuse techniques, and the implications of some attacks can be direct, such as the destruction of power, property, isolation of nations, demoralization, or loss of life. (Tabassum, Mustafa, & Maadeed, 2018).

Cyber Incidents in Qatar

In 2020, 18% of Qatari organizations suffered a cybersecurity incident, with 5% of organizations experiencing more than five incidents, costing an estimated average of $4.94 million each. (GBM, 2021). Cybercrime in Qatar caused an estimated economic loss of QAR 10 billion (US$2.7 billion) in 2021, with common cybercrimes including phishing, malware attacks, and ransomware attacks. In response, the Qatari government enacted a comprehensive cybercrime law in 2014, which considers various cyberattacks illegal, including unauthorized access to computer systems, data destruction, and online fraud. The Ministry of Interior established a dedicated cybercrime unit, tasked with investigating cyberattacks, prosecuting offenders, and promoting awareness about cyber threats. (Team Qatar Talk, 2023).

Qatar has experienced numerous cyberattacks in recent years due to its rapid internet penetration and transformation. In 2014, Qatar ranked first globally, with 91.5% of individuals using the internet. (Ministry of Transport and Communications, 2015). However, the country faces numerous cyberthreats, including the 2012 cyberattack on RasGas, a company that supplied LNG. Online criminals and civic hackers have targeted critical infrastructure and IoT devices. (Mills, 2012). The Syrian Electronic Army (SEA) has also launched cyberwars with Qatar, using Al Jazeera News to spread propaganda. Most users, with an average smartphone ownership of 2.8, are unaware of security issues. Qatar's average smartphone ownership is 2.8, but most users are unaware of security issues. The Syrian Pro-Battalion, which controls the Al Jazeera channel and broadcasts false information, exploits this to destabilize Qatar and its reputation.

(Al Jazeera, 2017). Qatar has experienced numerous and severe attacks from regional and national attackers, with the most recent being a ransomware attack on May 23, 2017, which made the Qatar News Agency website unavailable and displayed a scrolling ticker indicating support for extremists. This incident complicated Qatar's relationship with its brotherhood countries and initiated a blockade in the Gulf Cooperation Council (GCC). The cyberwar with Qatar has led to a pitiable situation, threatening authorities and undermining its security posture. (Qatar official State News Agency, 2017).

Hacktivist groups can operate throughout cyberspace, causing significant harm to organizations or nations they disagree with and enabling them to pursue their goals by illicit means, regardless of the attacker's nationality. In addition, there is a recent trend of using terrorism and wars to disparage, condemn, or attack a nation, its citizens, or its organizations. Sometimes, the motivation for cyberattacks is not financial gain, but rather defamation through the spread of false allegations. (Tabassum, Mustafa, & Maadeed, 2018). Qatari organizations face vulnerabilities due to outdated industrial control systems and a reactive approach to cybersecurity. To combat cybercrime effectively, cybersecurity must be a core function, controlled by a dedicated Security Operations Center and focusing on detection and response. Utilizing AI can help identify potential vulnerabilities before criminals exploit them. In order to avoid cybercriminals' breaches, organizations must prioritize cybersecurity. (GBM, 2021).

Methodology

Sample. The study sample consisted of 209 Qatari students, representing three Qatari universities. Of these, 163 (78%) were males, and 46 (22%) were females. Students (23%) reported being victims of cybercrimes, and 6% were perpetrators. The average time spent on the internet was 4 hours, with a standard deviation of 5.3.

Measurement

The study employed a survey as its research tool. The questionnaire included knowledge about the QCL scale (9 items with reliability Cronbach's alpha =.79), perpetration experience (8 items with reliability Cronbach's alpha =.86), victimization experience (8 items with reliability Cronbach's alpha =.83), and an attitude scale (29 items with reliability Cronbach's alpha =.96). All scales are based on a literature review. The Interval levels 0–5 categorize all scales, with 0 to 5 being the most common range.

Procedure and Data Collection

This quantitative study used the survey method on a sample of undergraduate students. The researchers provided informed consent to all students, requested their voluntary participation, and offered them the option to withdraw from the study at any time. The researchers also collected data by e-mailing the questionnaire to students for their completion.

Data Analysis

Data analyzed using descriptive statistical analyses and ANOVA. (using SPSS v. 21).

Findings

Knowledge about the Qatari Cyber Law (QCL)

Table 1 reveals that students' knowledge of GCL was below average, with the highest percentage of students learning about the QCL (66.5%), hearing about cybercrime convictions (56%), and observing behaviors in cyberspace that necessitated punishment (48.8%). Table 2 shows that online banking fraud was the highest crime students experienced on line (28%), DOS (17%), and ID theft (15%). Table 3 shows a small percent of students reported committing cybercrimes, mostly digital piracy (15%) and online banking fraud (10.5%).

Table 1 Students' responses on items of Knowledge in Cybercrimes

	Knowledge about QCL	Yes	No
	Have you read the Qatari Cybercrime Law (QCL)?	41.6	58.4
	Have you heard about the QCL?	66.5	33.5
	Have you watched a discussion about the QCL?	46.4	53.6
	Have you watched, read, or followed the House of Representatives discussion of the QCL?	23	77
	Have you seen behaviors on the network that require punishment?	48.8	51.2
	Have you participated in a network discussion that calls for punishment?	18.2	81.8
	Have you dealt with the QCL in a case?	19.6	80.4

	Have you heard of a conviction for violating the QCL?	56	44
	Do you know anyone who received a conviction under the QCL?	35.4	64.6

Table 2 Students' responses on items of victimization in cybercrimes

	Victimization exposure to cybercrimes	Yes	No
	Have you experienced the disablement of a website or email account due to data flooding (DoS)?	17	83
	Have you been a victim of a virus or computer worm that spread on the network (malware)?	12	88
	Have you ever purchased software, music, or movies knowing they were unauthorized or pirated by the network (digital piracy)?	13	87
	Have you been a victim of information or data theft from your computer (hacking)?	11	89
	Have you been a victim of using your personal information or account to obtain money or purchase things on your account (online banking fraud)?	28	72
	Has identity fraud used and exploited your information without your consent?	15	85
	Have you been a victim of an electronic crime against your race, religion, appearance, or country (hate crimes)?	11	89
	Have you been a victim of online harassment such as bullying, stalking, blackmail, threats or embarrassment, etc. (online harassment)?	9.5	90.5

Table 3 Students' responses on items of Perpetration in Cybercrimes

	Perpetration exposure to cybercrimes	Yes	No
	Have you ever intentionally used the Internet to spread a virus (malware)?	4	96
	Have you ever used the Internet to illegally access someone else's computer (hacking)?	6	94
	Have you ever tried to disable a website or email account by flooding it with data (DoS)?	5	95
	Have you downloaded software, music, or movies from the Internet knowing that they were illegal or pirated?	15	85
	Have you used the Internet to obtain a bank or credit card account for someone to get money or buy things (online banking fraud)?	10.5	89.5
	Have you sold something over the Internet without sending the product after receiving the money (online shopping fraud)?	5	95
	Have you ever used the Internet to send harmful messages on social media about race, religion, identity, etc. (hate speech)?	5	95
	Have you ever used the Internet to send messages with the intent to harass, such as bullying, stalking, blackmailing, or threatening someone (online harassment)?	6	94

Differences in perpetration exposure to cybercrimes

Tables 4 and 5 demonstrate that the average of students who did not experience perpetration, victimization, or knowledge about QCL was higher than that of those who did. Significant differences attributed to perpetration exposure (yes-no answer) were found in victimization experience (F = 26.470, α =.000), perpetration experience (F = 40.082, α =.000), and knowledge about QCL (F = 7.451, α =.007).

Table. 4 Descriptive statistics

Victimization experience	Groups	N	Mean	sd
	Yes	13	12.3846	3.45298
	No	196	14.9898	1.60764
	Total	209	14.8278	1.87314
Perpetration experience	Groups			
	Yes	13	13.1538	3.73823
	No	196	15.5765	1.01742
	Total	209	15.4258	1.45625
Knowledge about QCL	Groups			
	Yes	13	12.6154	2.93083
	No	196	14.5663	2.46632
	Total	209	14.4450	2.53402

Table 5 ANOVA table for the Gender Difference in Knowledge in QCL

	Source	Sum of Squares	df	Mean Squares	F	α
Victimization experience	Between Groups	82.743	1	82.743	26.470	.000
	Within Groups	647.057	207	3.126		
	Total	729.799	208			
Perpetration experience	Between Groups	71.556	1	71.556	40.082	.000
	Within Groups	369.544	207	1.785		
	Total	441.100	208			
Knowledge about QCL	Between Groups	46.403	1	46.403	7.451	.007
	Within Groups	1289.215	207	6.228		
	Total	1335.617	208			

Differences in victimization exposure to cybercrimes

Tables 6 and 7 demonstrate that the average of students who did not experience victimization was higher than that of those who did, both in terms of perpetration, victimization, and knowledge about QCL. Finally, ANOVA differences attributed to victimization exposure (yes-no answer) were found in victimization experience (F = 28.032, α =.000), perpetration experience (F = 13.355, α =.000), and knowledge about QCL (F = 7.804, α =.006) network that requires punishment.

Table. 6 Descriptive statistics

	Groups	N	Mean	sd
Victimization experience	Yes	48	13.6458	2.39227
	No	161	15.1801	1.52843
	Total	209	14.8278	1.87314
	Groups			
Perpetration experience	Yes	48	14.7708	2.31774
	No	161	15.6211	1.00588
	Total	209	15.4258	1.45625
	Groups			
Knowledge about QCL	Yes	48	13.5625	2.66503
	No	161	14.7081	2.44090
	Total	209	14.4450	2.53402

Table 7 ANOVA table for the Gender Difference in Knowledge in QCL

	Source	Sum of Squares	df	Mean Squares	F	α
Victimization experience	Between Groups	87.043	1	87.043	28.032	.000
	Within Groups	642.756	207	3.105		
	Toala	729.799	208			
	Between Groups	26.733	1	26.733	13.355	.000
Perpetration experience	Within Groups	414.367	207	2.002		
	Toala	441.100	208			
	Between Groups	48.525	1	48.525	7.804	.006
	Within Groups	1287.092	207	6.218		
Knowledge about QCL	Toala	1335.617	208			

Conclusion & Discussion

The study investigates the correlation between knowledge about Qatari cybersecurity law (QCL), victimization, and perpetration experience among Qatari students. Results show that students have average knowledge about GCL, with a high percentage hearing about QCL, hearing about cybercrime convictions, and witnessing punishment-requiring behaviors. However, only a small percentage of students commit cybercrime, mainly digital piracy. Significant differences were found in victimization experience, perpetration experience, and knowledge about QCL. The Routine Activities Theory provides a useful foundation for understanding the dynamics of situations that lead to cybercrime. RAT assists in explaining why particular people, systems, or organizations are more prone to falling victim to cybercriminals by recognizing motivated offenders, appropriate targets, and a lack of adequate guardianship. However, its implementation in the digital sphere requires careful consideration, especially given how online guardianship is evolving and how sophisticated cybercrime is. (Williams, 2016). Cybercrime in Qatar includes online fraud, identity theft, malware, phishing, cyberbullying, and cyber blackmailing. To report a cybercrime, users must log in to the Metrash2 app, select the department, attach a complaint photo, and send it for investigation. (Team Qatar Talk, 2023).

We interpret the findings in the context of Routine Activity Theory (RAT). The study looks at what causes cybercrime using some ideas from Routine Activity Theory (RAT). It says that people become victims of cybercrime when they are not properly protected by a likely cybercriminal and a good target in certain materials, historical times, and cyberspaces (Cohen and Felson, 1979). Cybercrimes such as malware infections and cybertheft victimization are associated with the Routine Activity Theory (RAT). Students lack of safety warnings, and online activities are some of the causes. However, cyberbullying may be less aware of its consequences, and online environments are not always accessible. (Abu Taher & Jahan, 2020).

The results revealed that students' knowledge and understanding of GCL was below average, while the majority only heard about QCL, heard about cybercrime convictions, and observed actions in cyberspace that necessitated punishment. The theory interprets this finding as a lack of legal and personal protection. A lack of legal knowledge is equivalent to the absence of a guardian. This condition requires the absence of a capable guardian, which can be a person or thing that discourages crime (cybercrime), both formal and informal. Cohen and Felson (1979) discovered that high-risk situations result in increased victimization, attractive targets, a lack of guardians, and motivated offender reach. (Williams, 2016).

Findings showed Online banking fraud, along with Denial of Service (DoS) and ID theft, was the most common online crime experienced by students. As Reyns study (2013) reveals, routine Internet access sites significantly influence online identity theft victimization, with frequent users of university and public computers experiencing higher victimization rates compared to workplace computers, suggesting low guardianship networks are more susceptible. Guedes, Martins, and Cardoso (2022) use the Routine Activity Theory (RAT) to investigate factors contributing to online identity theft victimization and fear. Data from a survey of university students and staff revealed that non-credit card users have lower odds of becoming victims, while those visiting risky content have higher odds. Socioeconomic status, education, and general crime fear explain the fear of OIT. Higher computer skills also reduce fear. (Guedes, Martins & Cardoso, 2022). (Reyns 2013). The National Cyber Security Program funds the UK's 'Cyber Street Wise' campaign, which promotes anti-virus installation, regular password changes, and discourages digital disengagement due to cybercrime anxiety. These security behaviors can be classified into three forms of individual capable guardianship: (1) passive physical guardianship; (2) active personal guardianship; and (3) avoidance personal guardianship. These security behaviors are regarded as the weakest links in the cyber security chain. (Gupta & Sharman 2011).

The findings revealed that the highest percentage of cybercrimes, which involve using personal information or accounts to obtain money or make purchases, were victims of online banking fraud and identity theft. The RA perceives Qatar as a high-income country. People anticipate wealth and possess valuable bank accounts. We expect people to be wealthy and store their money in bank accounts, making them valuable targets. Email, social engineering, and other methods can easily access these accounts. This is further reinforced by the lack of understanding among those involved in cybercrime law.

Smal percent of students reported committing cybercrimes, mostly digital piracy, and On line banking fraud. The RAT model applies to the cyber world, focusing on motivated offenders, suitable targets, and the absence of a capable guardian (Miro, 2014). The anonymity of the internet lowers the risk of apprehension, making criminal activities more attractive (Leukfeldt & Yar, 2016). Certain behaviors increase vulnerability, such as sharing personal information or using weak passwords. The lack of cybersecurity measures, such as anti-virus software and firewalls, also increases risks(Bossler & Holt, 2009). Cyberstalking is facilitated by motivated offenders targeting active social media or online platforms with limited supervision and privacy protections (Reyns et al., 2011). Financial scams often involve phishing emails or fraudulent websites, and individuals who lack proper training or digital defenses are more susceptible to falling victim to such scams. (Pratt et al., 2020). Digital identity theft is on the rise due to criminals exploiting online security vulnerabilities, particularly among those who share sensitive information without adequate protective measures. Digital identity theft is on the rise due to criminals exploiting online security vulnerabilities, particularly among those who share sensitive information without adequate protective measures. (Reyns, 2013).

Refrences

[1] Abu Taher, A. & Jahan, I., (2020) Causes of Cybercrime Victimization: A Systematic Literature Review. International Journal of Research and Review Vol.7; Issue: 5; E-ISSN: 2349-9788; P-ISSN: 2454-2237 89 Vol.7; Issue: 5; May 2020 Website: www.ijrrjournal.com pp 89-98

[2] Al Anzi, I. (2019). The role of educational institutions in raising awareness of the risks of cybercrime: a study of a sample of educational institutions for the university and secondary levels in the city of Riyadh. Journal of Security Research, 28(74), 13-79.

[3] Al Tamimi & Co., (. 2024). Cyber Crime Prevention Law in Qatar. https://www.tamimi.com/law-update-articles/cyber-crime-prevention-law-in-qatar/

[4] 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.

[5] Al-Badayneh, D., Al Dosari H., Al Qahtani, H., Alkhater, J., & Mehawesh, S., (2024). College Students Attributional Differences in Knowledge Awareness About

[6] 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

[7] Alrajeh SM, Hassan HM, Al-Ahmed AS, Alsayed Hassan D (2021) An investigation of the relationship between cyberbullying, cybervictimization and depression symptoms: A cross sectional study among university students in Qatar. PLoS ONE 16(12): e0260263. https://doi.org/10.1371/journal.pone.0260263

[8] AlZeben, G., AlKharabsheh, A., (2021). Cybercrimes and the awareness of its danger field study on Qatari university youth, Journal of the Islamic University of Human Research 29 (2). http://refhub.elsevier.com/S2405-8440(24)08402-0/sref27

[9] Al-Zoubi, M. (2023). "Crimes of Electronic Defamation, Libel, and Slander under Qatari Cybercrimes Law", International Review of Law, Volume 12, Regular Issue 1, pp 267-284. https://journals.qu.edu.qa/index.php/IRL/article/view/2964/1910

[10] Bamatraf, S. (2014). Assessing the Level of Knowledge About Cybercrimes Among Young Adults Within the United Arab Emirates Proceedings of The National Conference On Undergraduate Research (NCUR) 2014. University of Kentucky, Lexington, KY

[11] Bossler, A. M., & Holt, T. J. (2009). Online activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1), 400-420.

[12] Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

[13] Deora1, C., & Chudasama., D., (2021). Brief Study of Cybercrime on an Internet. Journal of Communication Engineering & STM Journals.

[14] Dou, G., Xiang, Y., Sun, X., & Chen, L. (2020). Link between cyberbullying victimization European Commission(2013). . Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; European Commission: Brussels, Belgium.

[15] Foody M, Samara M, El Asam A, Morsi H, Khattab A. A review of cyberbullying legislation in Qatar: Considerations for policy makers and educators. Int J Law Psychiatry. 2017 Jan 1; 50:45–51. https://doi.org/10.1016/j.ijlp.2016.10.013 PMID: 27837914

[16] GBM (2021). he Threat of Cyber Attacks. https://gbmqatar.com/insight/post/the-threat-of-cyber-attacks/

[17] Rehman, A., Shah, S. A. H., Nizamani, A. U., Ahsan, M., Baig, A. M., & Sadaqat, A. (2024). AI-Driven Predictive Maintenance for Energy Storage Systems: Enhancing Reliability and Lifespan. PowerTech Journal, 48(3). https://doi.org/10.XXXX/powertech.v48.113&#8203;:contentReference[oaicite:0]{index=0}

[18] Gohal, G., Alqassim, A., Eltyeb, E., Rayyani, A., Hakami, B., Al Faqih, A., Hakami, A., Qadri, A., & Mahfouz, M. (2023). Prevalence and related risks of cyberbullying and its effects on adolescents. BMC Psychiatry, 23, 39.

[19] Guedes I, Martins M, Cardoso CS. Exploring the determinants of victimization and fear of online identity theft: an empirical study. Secur J. 2022 Jul 21:1–26. doi: 10.1057/s41284-022-00350-5. Epub ahead of print. PMCID: PMC9302955.

[20] Gupta M. & Sharman R . (2011), Social and Human Elements of Information Security: Emerging Trends and Countermeasures . Information Science Reference .

[21] Holt, T. J., & Bossler, A. M. (2013). Examining the applicability of routine activities theory for cybercrime: A theoretical and empirical analysis. Crime and Delinquency, 60(4), 616-638.

[22] Ife, C., Davies, T., & Murdoch, S., (2019). Bridging Information Security and Environmental Criminology Research to Better Mitigate Cybercrime.

[23] Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Crime Science, 5(1), 1-12.

[24] Microsoft.(2012). Worldwide online bullying survey-Qatar [Internet]. Report No.: 2. Available from: file:///C:/Users/da18191/Downloads/WW%20Online%20Bullying%20Survey%20-%20Executive%20Summary%20-%20Qatar_Final%20(7).pdf

[25] McGuire, M. & Dowling, S., (2013).Improving the cyber crime evidence base (chapter 4). Home Office Research Report 75

[26] Mills, E., (2012). "Virus knocks out computers at Qatari gas firm RasGas, CNET.

[27] Ministry of Transport and Communications (2015). Qatar Ranks First on Two Significant Internet Penetration Indicators in the State of Broadband Report.

[28] Miro, F. (2014). Routine activity theory. The Encyclopedia of Theoretical Criminology.

[29] National Cyber Crime Reporting Portal. (2019). Retrieved November 24, 2023, from https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1703509

[30] 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)

[31] Purpura, P., (2013). Foundations of Security and Loss Prevention, Editor(s): Philip P. Purpura, Security and Loss Prevention (Sixth Edition), Butterworth-Heinemann, Pages 55-88, ISBN 9780123878465, https://doi.org/10.1016/B978-0-12-387846-5.00003-6. (https://www.sciencedirect.com/science/article/pii/B9780123878465000036)

[32] Qatar Official State News Agency (2017). Qatar official state news agency hacked, sensitive |News | DW | 24.05.2017."

[33] Jazeera (2017). Qatar's Al Jazeera website hacked by Syria's Assad loyalists." [Online]. Available: http://www.reuters.com/article/us-qatar-jazeerahacking/qatars-al-jazeera-website-hacked-by-syrias-assad-loyalistsidUSBRE8830ZI20120904.

[34] Regi, D., (2020). September 09, 2020. How to Report Cyber Crimes in Qatar? What are the Penalties for Perpetrators? https://qatarday.com/how-to-report-cyber-crimes-in-qatar-what-are-the-penalties-for-perpetrators

[35] Reyns, B. W. (2013), 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses', Journal of Research in Crime and Delinquency, 50: 216–38. doi:10.1177/0022427811425539.

[36] Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., & Kozych, I. (2021). Combating cybercrime: economic and legal aspects. Wseas Transactions On Business And Economics. DOI: 10.37394/23207.2021.18.72

[37] Tabassum, A., Mustafa, M., & Maadeed, S., (2018). The Need for a Global Response Against Cybercrime: Qatar as a Case Study. https://www.researchgate.net/publication/324031555_The_Need_for_a_Global_Response_Against_Cybercrime_Qatar_as_a_Case_Study

[38] Team Qatar's Talk, (2023). Qatar Guide Resources How To Report Cyber Crime In Qatar: A Step-by-Step Guide. https://www.qatarstalk.com/2023/12/23/how-to-reportشدد و العقوبات-cyber-crime/

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

[40] 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