SSHJ Everant ISSN-2456-2653
http://sshj.in/index.php/sshj/
Research Article
Social Science and Humanities Journal
CrossMark

Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case

[1*]Mohammed Faez Hasan, [2]Noor Salah Al-Ramadan

[1*]Asst. Professor, Department of Finance and Banking Sciences, Karbala University, Iraq

[2]Senior Lecturer, Department of Finance and Banking Sciences, Karbala University, Iraq

***Abstract*: -** *With the development of informational technology, criminals are using various cyberspaces to improve cyber-crime. Risk and cyber-attacks have developed into a major area of concern. As there has been an enormous increase in cyber-attacks, those attacks cause a series of damage to the critical banking process and caused huge financial losses to the system. To moderate cyber-crime and the cyber threat, financial industries seek to implement artificial intelligence and other cyber security to improve customer experiences and the banking process's efficiency. Thus, the current study came to assess and test the Iraqi banking experience with cyber attacks by unveiling the cyber security systems reaction towards the cyber attacks and whether the cyber attack promotes the intersystem of banks and motivates them to increase their precautions to save bank's databases and servers against violation. The study uses the questionnaire as a key tool to collect respondents' data on how to suffer from cyber attacks two years ago at least. The significant finding was that Iraqi private banks maintain a specific level of security regardless if there is a fierce attack or not. However, some respondents are still cautious about using online banking services due to Iraq's low security of public access to internet services.*

***Keywords*: -** *Cyber-attacks, Cyber Security, Hacking, Phishing, Private Banks,*

1. Introduction

The banking and financial sector is a large sector with a large number of customers around the world. During the year, the accessibility of banking services to the weakest or most vulnerable sections of society continued to grow(Anwar et al., 2021). According to the 2017 Findex globe database, it was found that there are 1.2 billion adults who have bank accounts. Furthermore, it has been seen that most countries are switching to the digital approach; about 51% prefer online banking channels while 26% access services through banks' websites and use mobile banking services. Due to the rapid growth of digitization in the bank, risk and cyber-attacks have developed into a major area of concern(Zhang et al., 2019). Over the last decades, there has been a humongous increase of cyber-attacks, and those attacks cause a series of damage to the critical banking process and caused huge financial loss to the system. It is crucial for the banking or financial sector to implement effective Cyber-security strategies such as artificial intelligence (AI) to cope with all these issues. Thus, the current study will shed light on the cyber security state in the Iraqi private banks and whether it offers an acceptable level to protect itself and keep its customers database.

2. Literature review

A cyber-attack can be defined as an attack that is propelled by the attackers with the help of more than one computer or network. Such kinds of attacks can intentionally affect the system as well as can steal data. This can be carried out by using compromised computers.

Cybercriminals adhere to a range of approaches to proposed cyber-attacks, including phishing, malware, ransom ware, denial of services, cross-side scripting, virus & Trojans, ATM/Debit/Credit card frauds, and many others more. Cyber-attacks are primarily designed to cause damage for profit,

disruption and revenge, and cyber warfare(Luo et al., 2018). In this regard, threat actors carry out so many practices to introduced cyber-attacks that largely depend on whether they are attacking a targeted or non-targeted entity. Furthermore, cybercriminals often generate software tools that assist them in using their attacks and often share them on the dark web to accomplish the goal. It often arises in initial level with detecting or scanning attackers looking for vulnerabilities or admission points that initiate the starting co-operation afterwards carry out the whole attack, whether it is to steal important information by deactivating the computer system or both.

A hacker can perform a cyber-attack in a number of ways to steal, modify or abolish data or evidence. In which the primary methods are denial of services, where DDoS attacks system resources so that it cannot return to service desires. But this is the only propelled since a huge number of other host machines are affected by malicious software organized by the attacker. The TCP SYN flood attack is another type of cyber-attack, in which attackers take advantage of buffer space usage through a mechanism of transmitting protocol session of a handshake. The device of attackers flood the goal the system of small ongoing line with the linking request, but when the target system replies to those, it does not respond(Yılmaz & Gönen, 2018). Thus, to deal with these attacks, the banking industry needs to have some securities.

2.1 Types of cyber attacks

While different monetary emergencies contrast in both their tendency and their seriousness, there are some normal conditions that commonly go with such emergencies. One is that a monetary emergency is frequently gone before by, joined by, or followed by periods where there are far reaching credit issues. The 2008 Global Financial Crisis was no exemption(Hasan et al., 2021). It was generally encouraged by a huge blast in subprime contract loaning, which made an enormous heap of home loan credits that were essentially ill-fated from the begin to wind up in default. Subprime contract advances are advances conceded to homebuyers with somewhat lower FICO ratings — to put it plainly, huge advances are given to individuals who will probably experience trouble making the advance instalments. As per a few investigations of monetary emergencies, the fast development of accessible credit, trailed by a more limited time of sharp credit fixing, often gives an early admonition sign of a coming monetary emergency. Monetary emergencies are almost constantly followed by a time of extreme credit fixing, where loan specialists try to check their danger openness by just stretching out acknowledge to borrowers for heavenly FICO assessments. Another reality about monetary emergencies is that despite the fact that they don't occur oftentimes, they do appear to happen with relative routineness. Over the previous century and a half or thereabouts, the United States has encountered by and large, some sort of monetary emergency about once every 25 to 30 years. Nonetheless, the latest history shows monetary emergencies emerging a bit more regularly. The U.S., for instance, experienced a significant securities exchange emergency in 1987, then, at that point, the website bubble in the mid-2000s, and afterward, the 2008 Global Financial Crisis. Monetary emergencies are frequently hard to anticipate, and one explanation is the way that the setting off cause might be a generally little occasion or series of occasions. For instance, the dab corn bubble that occurred around 2000-2002, while it was calamitous for some financial backers in the quickly developing tech industry, at first included a generally little extent of the general securities exchange. Despite the disappointment of various organizations, a few website organizations, like Amazon and Google, delighted in a monstrous development in the following years.

2.1.1 Cyber Stalking:

Cyber Stalking is the utilization of the internet or other electronic intends to follow somebody. This term is utilized reciprocally with online badgering and online maltreatment. Following by and large includes bothering or undermining conduct that an individual takes part in repeatedly, like after an individual, showing up at an individual's home or business environment, settling on badgering telephone decisions, leaving composed messages or

protests, or vandalizing an individual's property. Cyber Stalking is an innovatively based "assault" on one individual who has been designated explicitly for that assault for reasons of outrage, vengeance or control. Cyber Stalking can take many structures, including badgering, shame, and embarrassment of the casualty purging financial balances or other monetary control. For example, destroying the casualty's FICO rating irritating family, companions, and businesses to disengage the casualty the term can likewise apply to a "conventional" stalker who utilizes innovation to follow and find their casualty and their developments all the more effectively (e.g., utilizing Facebook warnings to realize what party they are joining in). A genuine digital stalker's expectation is to hurt their planned casualty utilizing the secrecy and untraceable distance of innovation. As a rule, the casualties never find the personality of the digital stalkers who hurt them, regardless of their lives being totally overturned by the culprit.

2.1.2 Hacking

"Hacking" is wrongdoing, which involves breaking frameworks and acquiring unapproved admittance to the information put away in them. Hacking had seen a 37 percent expansion this year. An instance of associated hacking with specific online interfaces and getting the private locations from the email records of city inhabitants had as of late become visible. Saltines are individuals who attempt to acquire unapproved admittance to PCs. This is regularly done using a 'indirect access' program introduced on your machine. Plenty of wafers additionally attempt to access assets using secret phrase-breaking programming, which attempts billions of passwords to track down the right one for getting to a PC (Stamp, 2011). Clearly, decent security from this is to change passwords consistently. In PC organizing, hacking is any specialized work to control the typical conduct of organization associations and associated frameworks. A programmer is any individual occupied with hacking. The expression "hacking" generally alluded to productive, sharp specialized work that was not really identified with PC frameworks. Today, be that as it may, hacking and programmers are most generally connected with pernicious programming assaults on the internet and different organizations. M.I.T. engineers during the 1950s and 1960s initially promoted the term and idea of hacking. Beginning at the model train club and later in the centralized server PC rooms, the supposed "hacks" executed by these programmers were expected to be innocuous specialized analyses and fun learning exercises. Afterward, outside of M.I.T., others started applying the term to less noteworthy pursuits. Before the internet became mainstream, for instance, a few programmers in the U.S. explored different avenues regarding techniques to change phones for settling on free significant distance decisions via telephone network unlawfully. As PC organizing and the internet detonated in prevalence, information networks became by a wide margin the most well-known objective of programmers and hacking.

2.1.3 Phishing

It is only one of the numerous fakes on the internet, attempting to trick individuals into leaving behind their cash. Phishing alludes to the receipt of spontaneous messages by clients of monetary organizations, mentioning them to enter their username, secret phrase, or other individual data to get to their record for reasons unknown. Clients are coordinated to a fake imitation of the first establishment's site when they click on the connections on the email to enter their data, thus they stay ignorant that the extortion has happened(Schiller et al., 2007). The fraudster then approaches the client's online financial balance and the assets contained in that record. Phishing is the demonstration of sending an email to a client dishonestly professing to be a set up real endeavour trying to trick the client into giving up private data that will be utilized for fraud. The email guides the client to visit a Web website where they are approached to refresh individual data, for example, passwords and Visa, federal retirement aide, and ledger numbers, that the genuine association as of now has. The Web webpage, be that as it may, is sham and set up just to take the client's data. For instance, 2003 saw the multiplication of a phishing trick in which clients got messages probably from

eBay guaranteeing that the client's record was going to be suspended except if he tapped on the gave interface and refreshed the Visa data that the veritable eBay previously had. Since it is somewhat easy to make a Web webpage seem as though a genuine associations website by impersonating the HTML code, the trick depended on individuals being fooled into speculation they were really being reached by eBay and were consequently going to eBay's webpage to refresh their record data. By spamming huge gatherings of individuals, the "phisher" relied on the email being perused by a level of individuals who really had recorded charge card numbers with eBay truly. Phishing, additionally alluded to as brand caricaturing or checking, is a minor departure from "fishing," the thought being that lure is tossed out with the expectations that while most will overlook the snare, some will be enticed into gnawing. Phishing is an email misrepresentation technique in which the culprit conveys genuine glancing email trying to assemble individual and monetary data from beneficiaries.(Jakobsson & Ramzan, 2008) Normally, the messages seem to come from notable and dependable Web locales. Sites that are often parodied by phishers incorporate PayPal, eBay, MSN, Yahoo, Best Buy, and America Online. A phishing undertaking, similar to the fishing trip it's named for, is a speculative endeavour: the phisher puts the draw expecting to trick somewhere around a couple of the prey that experience the trap. Phishers utilize various distinctive social designing and email parodying ploys to attempt to deceive

2.1.4 Cross-Site Scripting

Cross-Site Scripting (XSS) is a sort of PC security weakness regularly found in web applications that permit code infusion by noxious web clients into the pages saw by different clients. Instances of such code incorporate HTML code and customer-side contents. A took advantage of cross-site prearranging weakness can be utilized by assailants to sidestep access controls. Cross-Site Scripting assaults are a sort of infusion issue, in which vindictive contents are infused into the generally kind and believed sites. Cross-Site Scripting (XSS) assaults happen when an assailant utilizes a web application to send noxious code, by and large as a program side content, to an alternate end client. Blemishes that permit these assaults to succeed are very inescapable and happen anyplace a web application utilizes contribution from a client in the yield it produces without approving or encoding it(Milhorn, 2007). An assailant can utilize XSS to send vindictive content to a clueless client. The end client's program has no real way to realize that the content ought not be trusted and will execute the content. Since it thinks the content came from a confided in source, the noxious content can get to any treats, meeting tokens, or other touchy data held by your program and utilized with that site. These contents can even change the substance of the HTML page.

2.1.5 Distributed DoS attacks

Appropriated DoS assaults (DDoS) are a sort of cybercrime assault that cybercriminals use to cut down a framework or organization. Now and again, associated loT (web of things) gadgets are utilized to dispatch DDoS assaults.

A DDoS assault overpowers a framework by utilizing one of the standard correspondence conventions it uses to spam the framework with association demands. Cybercriminals who are doing cyber extortion might utilize the danger of a DDoS assault to request cash. Then again, a DDoS might be utilized as an interruption strategy while other sort of cybercrime happens.

A popular illustration of this sort of assault is the 2017 DDoS assault on the UK National Lottery site. This brought the lottery's site and versatile application disconnected, forestalling UK residents from playing cybercrime that compromises protection Cybercrime disregards people's protection and the security of their information, especially hacking, malware, wholesale fraud, monetary extortion, clinical misrepresentation, and certain offenses against people that include the noteworthy of individual data, messages, pictures, and video and sound accounts without people's assent or consent (e.g., cyber stalking, cyber harassment) Data is viewed as a ware on the web and disconnected by both lawful and illicit

entertainers (Thijeel et al., 2018). Consequently, information is an essential objective of cybercriminals. Information likewise assumes a necessary part in the commission of numerous cybercrimes, fundamentally on the grounds that it isn't satisfactorily ensured and can be unlawfully gotten to and acquired. Information breaks have come about because of lost or taken encoded streak drives and other capacity gadgets (principally PC and cell phones), helpless framework and information security, unapproved admittance to the data set or the surpassing of approved admittance to a data set, and inadvertent revelation, delivery or distribution of information.

2.2. Cyber securities in bank

Cyber-security has been of great importance in the financial sector. From scratch, it becomes necessary to cultivate trust and credibility. There are so many reasons cyber-security is important in the banking industry, for example, everyone is going cashless using digital money via debit and credit cards. In this context, it becomes essential to ensure that all cyber-security measures are in place, to protect data and privacy. A survey reveals that the cost of cybercrime in the global economy in 2016 was $ 5450 billion, with an Asian organization counting more than $ 81 billion requests (Werner et al., 2017). Denial of services, infrastructure attacks, and other data protection issues are essential parts of high-profile cyber-attacks. About 70% of capital market and banking CEOs believe cyber-security is a threat to their development. Security incidents impacted the organization of financial services 300 times more frequently than activities in various industries. While large companies are more targeted.

To cope with this situation, it is vital to create some securities programs. In one year, the global banking and financial industries say the cyber-attacks cost about $ 360 billion. To combat this challenge, many bankers are trying to implement artificial intelligence. Nevertheless, for a company, there is no precise way to avoid a cyber-attack but to reduce the risk the bank can follow some best practices on cyber securities(Zhou et al., 2020). Therefore, the execution of the defence perimeter such as firewalls that assist in blocking attempts of attacking by using software such as antivirus, etc. helps to cope with this situation

2.3. Combating challenges in the bank.

The fast development of commuting technology is made up of many positive factors; however, these technologies also create a problem. Where the most common problems are fraud and theft with the help of information technology. The number and cybercrime are increasing day by day and it has just jumped into second position as an economic crime and the most reported financial institutions as a main target. These are done by information technology and monitoring, control, detachment, and prevention become very difficult. Few cyber-attacks impose direct impacts on banking or organizational systems such as phishing. It is not easy to detect this kind of attack and mitigate this problem.

Advances in automation and security integration are analysed and several products are able to profile key benefits. Response time is identified correctly, along with these scarce resources are involved in improving the productivity of talented security engineers. Thus, with the help of artificial intelligence evolving threats can be identified by collecting responses of banks towards cybercrime. It is important to assess the implementation of artificial intelligence in order to provide high-quality cyber security in a bank as it maintained the ultimate budget (Saha et al., 2018).

There are so many cyber-security threats in the banking industry, the most common being identity theft, spoofing, and insecure third-party services. To mitigate all of these threats, the banking industry can make sure it has the right security solution by educating employees so that they can regularly check the entire system. Therefore, the banking sector has so many opportunities to improve its cyber-security despite its vulnerability.

Banks need to increase their forward-looking approach to cyber-security. Preventive measures already in use, including firewalls, antivirus and anti-malware applications, and vulnerability scanning. Though, by implementing some other

intelligence measures such as artificial intelligence (AI) implemented in the first authentication with the help of biometric access for multi-factor authentication (MFA), the defends can be strengthened. For example, using a fingerprint to verify a payment with a digital wallet such as Apple Pay or Google Pay. (Kavousi-Fard et al., 2021).

The main cyber-security challenges are the inherent vulnerability of the system and software used by the bank's countless access points to intentional and outdated defence technologies that are highly vulnerable to advanced attack technologies used by hackers. However, mandatory cyber-security preparedness is the most basic objective of the banking institution. The growing adoption of social media leads to greater potential for hackers to exploit. Many users post their data or anyone who sees it(Kalech, 2019). Which can potentially be exploited to attack user organizations. Using social media to spread fake news can have an insidious impact on banks' reputations. Prior to the development of the chatbots, chatbots research for the customer service map was conducted successfully.

2.4. Combating or Precautions

All in all, presently, you comprehend the danger cybercrime addresses, what are the ideal approaches to ensure your PC and your own information? Keep programming and working framework refreshed Keeping your product and working framework forward-thinking guarantees that you profit with the most recent security patches to ensure your PC(Hasan & Al-Dahan, 2019) . Utilize hostile to infection programming and keep it refreshed Using against infection or a complete web security arrangement like Kaspersky Total Security is a shrewd method to shield your framework from assaults. Against infection programming permits you to check, distinguish and eliminate dangers before they become an issue. Having this security set up assists with shielding your PC and your information from cybercrime, giving you piece of brain. In the event that you utilize against infection programming, ensure you keep it refreshed to get the best degree of insurance. Utilize solid passwords be certain to utilize solid passwords that individuals won't figure and don't record them anyplace. Or then again utilize a respectable secret word chief to create solid passwords haphazardly to make this simpler(Erickson, 2008). An illustration of a solid secret phrase is "Animation Duck-14-Coffee-Glvs". It is long, contains capitalized letters, lowercase letters, numbers, and unique characters. It is a special secret word made by an arbitrary secret key generator and it is not difficult to recollect. Solid passwords ought not to contain individual data. Never open connections in spam messages an exemplary way that PCs get tainted by malware assaults and different types of cybercrime is by means of email connections in spam messages. Never open a connection from a sender you don't have a clue (Flayyih et al., 2018). Try not to tap on joins in spam messages or untrusted sites another way individuals become casualties of cybercrime is by tapping on joins in spam messages or different messages, or new sites. Try not to do this to remain safe on the web.

Try not to give out close to home data except if secure Never give out close to home information via telephone or through email except if you are totally certain the line or email is secure. Verify that you are addressing the individual you think you are. Contact organizations straightforwardly about dubious solicitations if you get requested information from a called organization you, hang up. Get back to them utilizing the number on their authority site to guarantee you are addressing them and not a cybercriminal. In a perfect world, utilize an alternate telephone in light of the fact that cybercriminals can hang tight open. At the point when you think you've re-dialled, they can claim to be from the bank or other association that you believe you're addressing. Be aware of which site URLs you visit keep an eye on the URLs you are tapping on. Do they look genuine'? Try not to tap on joins with new or malicious looking URLs. In the event that your web security item incorporates usefulness to get online exchanges, guarantee it is empowered prior to doing monetary exchanges on the web. Watch out for your bank proclamations our tips should assist you with trying not to fall foul of cybercrime. Notwithstanding, as a last resort, detecting that you have become a casualty of

cybercrime rapidly is significant. Watch out for your bank articulations and question any new exchanges with the bank. The bank can examine whether they are deceitful.

3. Methodology

3.1 Data and sample

Due to the lake of dataset regarding cyber-attacks within Iraqi private banks, the study depended on questionnaire methodology to collect the data pertaining the main variables. The date acted the respondents as the banks' customers how to encounter one cyber-crime at least two years ago. The sample covers middle Iraqi cities (Baghdad, Karbala, Babel, and Najaf), and consists of (51) responses. The male comprises (62.7%) while the female is about (37.3%), which is also mentioned in Table1. The age groups showed in Table 2, while the experience of respondents appeared in Table 3.

Table 1: Gender statistics of the sample

Gender	Frequency	Percent
Male	32	62.7
Female	19	37.3
Total	51	100.0

Table 2: Age statistics of the sample

Age Range	Frequency	Percent
26-35	14	27.5
36-45	26	51.0
46-55	8	15.7
56 and above	3	5.9
Total	51	100.0

Table 3: Experience statistics of the sample

	Frequency	Percent
1-3	3	5.9
4-6	27	52.9
7-9	18	35.3
10-12	3	5.9
Total	51	100.0

3.2. Study tool design and reliability

The study is based on the questionnaire as the main tool, which is designed according to the literature review of current-study variables and experts in the field. The independent variables namely (Cyber Stalking, Hacking, Phishing, Cross-Site Scripting, and Distributed DoS attacks), whilst the dependent variable represented by (Cyber security readiness) as the sole variable involve eight questions items. Each independent variable has four items as questions for respondents. The questionnaire used a Likert five-point scale.

To confirm the reliability of the study tool (questionnaire), the Cronbach's alpha coefficient applied, besides calculating variance inflation factor (VIF), which appear in Table 4, the result manifests that Cronbach's alpha value equals to (0.78), which refers that internal consistency of the study tool is marked "good". This covers all the 28 items in the questionnaire. On the other hand, The VIF results appear less than 2.5, which means there is no multicollinearity problem among the variables when multiple regression is applied. Those scales support the validity and reliability of the study tool for measuring the variables of the study.

Table 4: variance inflation factor (VIF) values of independent variables

Dependent Variable With-	Collinearity Statistics	
	Tolerance*	VIF
Cyber stalking	.890	1.124
Hacking	.884	1.131
Phishing	.869	1.151
Cross site script	.927	1.079
Distributed DoS attacks	.816	1.226

Note: VIF calculated by 1/Tolerance

4. Result and Discussion

To find the desired results, the statistical analysis covers the descriptive statistics for each variable and is accompanied by Correlation and multiple regression to unveil the relationships among the study's variables.

4.1. Descriptive statistics of Variables

Understanding each variable requires finding out and interpret underlying items results. Therefore, here the descriptive statistics measures were presented, respectively.

4.1.1 Cyber Stalking results

Table 5, point out that the mean of this variable is (3.5539). In addition, all the underlying items were over three. This implies the existence of cyber stalking attacks and customers face harassment and threats to a slight level while doing banking services via PC or mobile phone. Likewise, sometimes there was a threat of transfer money through a bank account or credit card to settle an electronic blackmail matter.

Table 5: Cyber Stalking descriptive statistics of respondents

item	N	Minimum	Maximum	Mean	Std. Deviation	Variance
cyber_stalking1	51	2	5	3.53	.674	.454
cyber_stalking2	51	2	5	3.59	.698	.487
cyber_stalking3	51	2	5	3.65	.627	.393
cyber_stalking4	51	2	5	3.45	.702	.493
Cyber Stalking*	51	2.75	4.50	3.5539	.38508	.148

*Note: means this is the total of the dimension

4.1.2 Hacking results

In turn, this variable well-known to common people, therefor technology developed many strategies and technical solutions to encounter such kind of attacks. However, the respondents report that they feel unsafe because of possibility to such attack. Particularly, through the smartphone untrusted application or from connecting to public wireless network where there is low privacy and hackers may exist. Accordingly, the Table 6 manifest the mean of this variable which was (3.3382) and only first item was under (3) because it is uncommon the customers lose access to their banking services account because of login credentials hacking.

Table 6: Hacking descriptive statistics of respondents

	N	Minimum	Maximum	Mean	Std. Deviation	Variance
hacking1	51	2	4	2.90	.671	.450
hacking2	51	2	4	3.24	.710	.504

hacking3	51	2	5	3.98	.735	.540
hacking4	51	2	5	3.24	.839	.704
Hacking(Total)	51	2.75	4.25	3.3382	.38021	.145

4.1.3 Phishing results

According to the result of Table 7, this variable achieved value (3.4951) as arithmetic mean, which implies the support of the existence of phishing. All items were achieved mean by more than three (except item four), which means that most of the customers confronting a type of phishing like receiving fake links offers to send login credentials or fake email requires money transfer or their security software alerts for suspicious or malicious links. In contrast, the customers refuse to admit whether they feel safe while performing their online banking activities and that attributed to that perpetrator may ambush the website or routes of banking activities previously.

Table 7: Phishing descriptive statistics of respondents

	N	Minimum	Maximum	Mean	Std. Deviation	Variance
phishing1	51	2	5	4.27	.918	.843
phishing2	51	2	5	4.06	.732	.536
phishing3	51	2	4	3.08	.595	.354
phishing4	51	2	3	2.57	.500	.250
Phishing(Total)	51	2.50	4.25	3.4951	.32592	.106

4.1.4 Cross-site script results

All customers asserted that they usually click on fake banners or links that transfer them to suspicious external links while they are browsing the internet or the notified by their security software about unsafe and malicious links or content. Consequently, this variable has mean value of about (3.5686) which is over three, and therefore this confirms the availability of such types of attacks within the under-study banking environment. For more support, all items recorded more than three in terms of the arithmetic mean. The results of this variable is appear in the Table 8.

Table 8: Cross site script descriptive statistics of respondents

	N	Minimum	Maximum	Mean	Std. Deviation	Variance
cross_site_scripting1	51	3	5	3.88	.683	.466
cross_site_scripting2	51	3	5	3.92	.717	.514
cross_site_scripting3	51	2	4	3.31	.510	.260
cross_site_scripting4	51	2	4	3.16	.543	.295
Cross site script (Total)	51	3.00	4.25	3.5686	.28319	.080

4.1.5 Distributed doS attacks results

Table 9 obviously show, that even though this variable attends clearly among respondents with obvious mean reach to (3.2809), but this attributed to customers worry about bank ability to protect their information and privacy appropriately. Thus, they agree with these variable items as long as no violation happens to their account's credentials tell now. Hence, the arithmetic means already excess three, which represent the study standard mean.

Table 9: Distributed doS attacks descriptive statistics of respondents

	N	Minimum	Maximum	Mean	Std. Deviation	Variance
distributed_doS_attacks1	51	2	5	3.33	.683	.467
distributed_doS_attacks2	51	2	5	3.12	.993	.986
distributed_doS_attacks3	51	2	5	3.18	.932	.868
distributed_doS_attacks4	51	0	5	3.50	.758	.575

Distributed doS attacks (Total)	51	2.58	4.50	3.2809	.40236	.162

4.1.6 Cyber security readiness results

Cyber security readiness stands for the lone dependent variable in the study. Table 10, show that the arithmetic mean of each item, besides the total mean, was over three. This implies the respondents have similar answers about banks' ability to protect customers' data and maintain cyber security applications with strict policy. In addition, the banks follow a specific plan to encounter sudden attacks if it happens an anytime with continues technical support and advisory services.

Table 10: Cyber security readiness descriptive statistics of respondents

	N	Minimum	Maximum	Mean	Std. Deviation	Variance
cybersecurity_readiness1	51	3	5	3.65	.522	.273
cybersecurity_readiness2	51	2	5	3.76	.862	.744
cybersecurity_readiness3	51	3	5	3.57	.608	.370
cybersecurity_readiness4	51	3	5	3.76	.681	.464
cybersecurity_readiness5	51	3	5	3.73	.750	.563
cybersecurity_readiness6	51	2	5	3.51	.703	.495
cybersecurity_readiness7	51	2	5	3.71	.782	.612
cybersecurity_readiness8	51	3	5	3.92	.717	.514
Cyber security readiness(Total)	51	3.25	4.25	3.7010	.27051	.073

4.2. Correlation and regression of the variables

Apparently, from Table 11 we can assert that some variables show a negative correlation coefficient, but all variables manifest weak and insignificant relationships. Whereas the dependent variable (Cyber security readiness) did not achieve any positive correlation with any independent variable, furthermore, related negatively with (Hacking), this was insignificant, anyway. This state is similarly still the same among independent variables. This implies that there is no statically significant relationship between independent variables and the study's dependent variable. In addition, the independent variables did not show any interrelationship, which confirms that no collinearity problem exists.

Table 11: Correlation matrix of study variables

	Cyber Stalking	Hacking	Phishing	Cross site script	Distributed doS attacks
Hacking	0.044*				
Sig.	(0.761)**				
Phishing	-0.107	-0.158			
Sig.	(0.453)	(0.269)			
Cross site script	0.16	-0.069	0.153		
Sig.	(0.261)	(0.631)	(0.285)		
Distributed doS attacks	-0.215	-0.266	-0.174	0.061	
Sig.	(0.13)	(0.059)	(0.221)	(0.67)	
Cybersecurity readiness***	0.002	-0.261	0.068	0.183	0.06
Sig.	(0.99)	(0.064)	(0.635)	(0.197)	(0.675)

Note: *correlation according to Pearson correlation,

** Significance (P-value) was for two tail hypothesis and degree of freedom is (50).

*** Dependent variable

As a next step, multiple regression has been applied to address the form of relationship and test withier it is possible or not. Table 12 previews the model

summary of multiple-regression of the study model, which reveal that it is difficult to use the study model to shape the relationship among the study variables because of very weak (R^2) value which indicate that independent variables could not show clear or significant impact over the dependent variable. Therefore the regression model could not be recognized as a guide for the impact, notwithstanding that the Durbin-Watson value was (2.295), which is slightly above two, and this indicates there is no autocorrelation among the model residuals.

Table 12: Model summary of multiple regression

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.310	.096	-.004	.27107	2.295

Whereas Table 13 show that the model is insignificant on account of model significance (P-value) was (0.453) and it was more than (0.05). As a result, there is no influence for an independent variable over the Cybersecurity readiness even if the model was referred to a relationship, thus the independent variables could not be valid to interpret the changes that happen to Cybersecurity readiness in this sample at least.

Table 13: ANOVA results of multiple regression model

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.352	5	.070	.959	.453[b]
	Residual	3.307	45	.073		
	Total	3.659	50			

5. Conclusions

Under the current state around the world, the impact of the pandemic and its development affects all the business sectors and applies an enormous tension over people by lowering their income. As a result, the cyber-attacks increased globally to bring new challenges to all institutions and especially for banks and financial institutions. Therefore, our study is coming as try to unveil the level of cybersecurity readiness in Iraqi private banks. Consequently, the study revealed that customers encounter cyberattacks sometimes, and they still worry about such type of crime. At the same time, the Iraqi private banks do their best to update and built up their cybersecurity systems, either there are cyberattacks or not. Because cybersecurity becomes a contemporary issue in our time, however, these possibilities are still subject to the bank budget and experience in terms of protecting their customers' credentials and internal system servers from violation.

References

1. Anwar, N., Hasan, M. F., & Nasim, J. (2021). Role of Islamic Teachings in Shaping Mental Health of Educated Youth : A Contribution towards Good Governance. International Journal of Social Science, Innovation and Educational Technologies, 2(7), 203–214.
2. Erickson, J. (2008). Hacking: The Art of Exploitation, 2nd Edition. In Assembly. No starch press. http://www.amazon.com/Hacking-Art-Exploitation-Jon-Erickson/dp/1593271441
3. Flayyih, H. H., Ali, S. I., & Mohammed, Y. N. (2018). The Effect of Integration of Coroprate Governance Mechanisms and Audit Quality in Earning Management : An Empirical Analysis of Listed Banks in Iraqi Stock Exchange. International Journal of Engineering & Technology, 7(4), 337–344.
4. Hasan, M. F., & Al-Dahan, N. S. (2019). The herding effect of domestic investors on foreign investors: Evidence from the Iraq stock exchange. International Journal of Innovation, Creativity and Change, 10(6), 234–245.
5. Hasan, M. F., Hadi, H. S., & Jasim, N. A. H. (2021). The Validity of Altman's Models in Predicting Iraqi Private-Banks Soundness. JOURNAL OF MANAGEMENT AND

ACCOUNTING STUDIES, 9(01), 79–89. https://doi.org/https://doi.org/10.24200/jmas.vol9iss01pp79-89

6. Jakobsson, M., & Ramzan, Z. (2008). Crimeware: understanding new attacks and defenses. In Techniques. Addison-Wesley Professional. http://www.amazon.com/dp/0321501950

7. Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. Computers and Security, 84, 225–238. https://doi.org/10.1016/j.cose.2019.03.007

8. Kavousi-Fard, A., Su, W., & Jin, T. (2021). A Machine-Learning-Based Cyber Attack Detection Model for Wireless Sensor Networks in Microgrids. IEEE Transactions on Industrial Informatics, 17(1), 650–658. https://doi.org/10.1109/TII.2020.2964704

9. Luo, X., Yao, Q., Wang, X., & Guan, X. (2018). Observer-based cyber attack detection and isolation in smart grids. International Journal of Electrical Power and Energy Systems, 101, 127–138. https://doi.org/10.1016/j.ijepes.2018.02.039

10. Milhorn, H. T. (2007). Cybercrime: How to Avoid Becoming a Victim. Universal-Publishers. http://books.google.com.my/books?id=MDziocPjoz0C

11. Saha, S., Roy, T. K., Mahmud, M. A., Haque, M. E., & Islam, S. N. (2018). Sensor fault and cyber attack resilient operation of DC microgrids. International Journal of Electrical Power and Energy Systems, 99, 540–554. https://doi.org/10.1016/j.ijepes.2018.01.007

12. Schiller, C., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C., & Cross, M. (2007). Botnets: The Killer Web Applications. In Syngress Publishing. Elsevier.

13. Stamp, M. (2011). Information security: principles and practice. John Wiley \& Sons.

14. Thijeel, A. M., Flayyih, H. H., & Talab, H. R. (2018). The relationship between audit quality and accounting conservatism in the Iraqi banks. Opcion, 34(Special Issue 15), 1564–1592.

15. Werner, G., Yang, S., & McConky, K. (2017). Time series forecasting of cyber attack intensity. ACM International Conference Proceeding Series, 1–3. https://doi.org/10.1145/3064814.3064831

16. Yılmaz, E. N., & Gönen, S. (2018). Attack detection/prevention system against cyber attack in industrial control systems. Computers and Security, 77, 94–105. https://doi.org/10.1016/j.cose.2018.04.004

17. Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Transactions on Industrial Informatics, 15(7), 4362–4369. https://doi.org/10.1109/TII.2019.2891261

18. Zhou, Q., Shahidehpour, M., Alabdulwahab, A., & Abusorrah, A. (2020). A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids. IEEE Transactions on Smart Grid, 11(5), 3690–3701. https://doi.org/10.1109/TSG.2020.2979160