AL KUT JOURNAL OF ECONOMIC AND ADMINISTRATIVE SCIENCES
Publisher: College of Economics and Management - Wasit University

The Financial costs of cyber breaches with reference to Iraqi procedures

Asst. Prof.Muhannad Khalifa Obed[1]

University of Fallujah – College of Administration and Economics

dr.muhannadkhalifa@uofallujah.edu.iq

https://orcid.org/0000-0003-4348-7835

Dr. Adel Mansour Fadel Al-Issawi[2]

Department of Financial and Banking Sciences

College of Administration and Economics /Al-Iraqia University Official

adel.m.fadel@aliraqia.edu.iq

Abstract:

The research aims to analyze the costs of cyberattacks and their breaches globally, and to identify the legislation and procedures followed in Iraq to combat them. A distinction exists between developed and developing countries regarding cyberattacks, particularly those targeting banks, which are not confined to specific geographical boundaries. Courts apply the provisions of the Iraqi Civil Law No. 40 of 1951. The Iraqi Council of Representatives approved a new draft law to combat cybercrimes in 2020. The 2020 law did not include any substantive amendments, given the continuous evolution in cybercrime technology. Confronting these challenges requires recruiting more advanced technical units, intensifying efforts to enhance and develop a comprehensive cybersecurity strategy, improving national capabilities, and adopting new legislation.

Introduction:

Today, the world is witnessing rapid digital transformation across all sectors. According to recent reports, breaches and financial costs are rising due to increasingly sophisticated cyberattacks, making cybersecurity an utmost necessity. These attacks range from simple attempts to steal personal data to large-scale assaults targeting nations' critical infrastructure. As technological devices advance, they become more vulnerable and complex—especially in sensitive financial sectors like banking due to the critical information they handle. Faced with these breaches and the incurred global costs, it is imperative for Iraq and its financial institutions to adopt effective legislation and technology to strengthen cybersecurity.

Research Problem: Financial institutions in Iraq suffer from weak cybersecurity infrastructure and a lack of effective, enforced legislation to counter cyberattacks, leading to increased security and economic costs.

The importance of research: The significance of this research lies in proposing precautionary measures for information and digital elements within information systems, as outlined in Iraqi legislation and the Central Bank of Iraq's policies. This is crucial given the substantial global financial losses incurred. Cybersecurity requires a cohesive framework to ensure a comprehensive approach and assess the scale of cyber-related costs.

Research Objectives:

1. Analyze global costs and breaches resulting from cyberattacks.

2. Outline existing legislation and steps taken in Iraq to counter cyber threats.

3. Propose solutions to mitigate losses and enhance cybersecurity in Iraq.

Keywords: Financial costs, Cyber breaches, Iraqi measures

First: Breach Operations

Also known as data breaches or data leaks or information leaks. The process of a data breach is classified into four stages, which are:

1. Reconnaissance: The hacker attempts to find a loophole or ambiguity in the system that would allow them to target a specific set of data.

2. Attack: The hacker seeks to build a friendly relationship with the victim to dispel any doubts about the possibility of a data breach.

3. Social or Network Attack: The first type occurs when the hacker attempts to penetrate a network or organization by exploiting its vulnerabilities. It involves deceiving people, either by gaining their trust in advance or indirectly by granting them access to networks or systems.

4. Extraction: Without extraction, the final step in the data identification process, a hacker can easily access sensitive information. (Senbaghavali Al-Abd Al-Ghafi, 2022:5)

Electronic breach has numerous impacts. Direct economic effects include the immediate costs resulting from a cyber attack, including the costs of recovering IT systems, legal expenses, fines, compensation for affected customers, and direct financial losses. For instance, Direct costs include IT repairs, fines, incident response expenses, and legal fees. For example, data breaches result in average costs of $4.24 million per breach. Based on recent industry reports, ransomware attacks cost an average of $1.85 million per breach, including ransom costs and system recovery expenses (Federico, 2024:475).

According to studies, the banking sector is the most affected by electronic breach operations because it is a rich source of valuable data and has weak security defenses in banking and financial institutions (Alismai & Shehab, 2024:170).

International experiences indicate a rise in cyber attacks due to weaknesses in the banking sector, which has led to impacts on financial institutions in the following ways:

1. Cybercriminals can remotely access systems to manage all data.

2. They can cause financial loss (by conducting fraudulent transactions).

3. They can steal confidential information and sell it, or even use it for espionage or terrorism purposes.

4. They can target customers by attacking the institution, which may lead to customer frustration or identity theft.

5. The institution's public image may be damaged due to insufficient compliance with information security (NIDA, 2018:2-7).

The New York Times reported that a cyber attack in 2012 angered customers of Bank of America, Chase, Citigroup, Wells Fargo, and PNC Bank, who were unable to access their accounts. The bank could not explain the circumstances of the incident or what happened in detail. However, the CEO revealed to analysts that the bank spends millions of dollars annually on cybersecurity to protect against data breaches and that this was a case of denial-of-service, aimed at causing the institution financial losses.

In the United States, it was announced that the Yahoo breach affected 3 billion customer accounts, and the Equifax breach in 2017—which affected 143 million customers—was the largest discovered breach ever. According to the 2017 cyber attack report. And according to MailGuard, the most common cyber crimes in 2017 were the malware WannaCry, NotPetya, and KRACK (Vergara & Cakir, 2024:9).

In 2020, the United Kingdom succeeded in thwarting attacks worth 19 million pounds, and as a result, individuals were identified and arrested, due to the use of malicious computer software (Trojan horses) that infiltrated computer programs (Alismay and Shahab, 2024: 172).

Additionally, 50% of companies in the UK experienced some form of cyber attack in 2023. Nearly one billion email messages were exposed in one year, affecting one in five internet users. https://aag-it.com/the-latest-cyber-crime-statistics.

In the banks of Sweden, fraud was committed by mail (rakin.zip or raking.exe) and the identities of 250 people were stolen, and $1.5 million was stolen in Sweden (Alismai & Shehab, 2024: 172).

In Nigeria in 2013, online security breaches targeting financial institutions increased by more than 30% between 2015 and 2017. Thus, cybersecurity breaches have become a phenomenon that has impacted the banking sector. Furthermore, there is no standardized method for measuring the financial cost of these breaches (Harrison and Wang, 2019:9).

A worrying statistic is that 67% of SMBs lack the internal skills needed to understand a data breach. This problem is easing as the number of SMBs using managed cybersecurity service providers increases; the percentage reached 89% as of 2022, compared to 74% in 2020.

The COVID-19 pandemic has impacted cybersecurity, and companies have decided to quickly transition to remote working. Cybercriminals have exploited network disruptions and security vulnerabilities during these transitions. Malware attacks increased in 2020 by 358% compared to 2019. Cybercrime statistics for 2019 show that the number of victims reached 53 per hour. In 2020, the number of victims per hour rose to 90, a 69% increase. https://aag-it.com/the-latest-cyber-crime-statistics

Globally, over the past decade, most sectors have witnessed an increase in the level of cyber breaches, with the banking and financial institutions sector being the most affected. Table (1) shows that the peak occurred in 2020., with 664 breaches recorded and 17.94 million records leaked. The year 2019 saw a significant jump compared to 2018 (from 368 to 510 breaches). That is, in 11 years, 3,697 breaches were recorded, resulting in 99.96 million records leaked.

Among the reasons for the escalating pace of breaches are increased reliance on technology in 2020, in addition to reliance on cloud storage. This has provided hackers with advanced methods for breaching.

Table (1) Number of breaches in financial institutions for the period 2010-2020

Year	Number of data breaches	Millions of records exposed
2010	195	5.27
2011	215	5.81
2012	221	5.95
2013	277	7.47

2014	310	8.37
2015	265	7.30
2016	322	8.70
2017	350	9.45
2018	368	9.94
2019	510	13.76
2020	664	17.94
Total	3697	99.96

Source: Shihab, Rami, Al-Ismaili, Abrar, et al. (2024) Cybersecurity Risk Assessment on Banking Services, Journal of Internet Services and Information Security, Vol. 14, No. 3, p. 184.

Table (2) shows the breaches suffered by financial institutions as a result of cyber attacks.

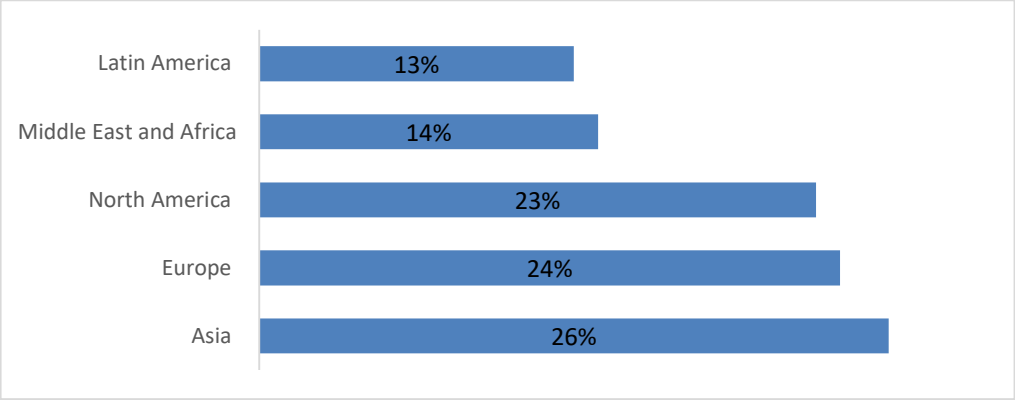
Table (2) Cyber breaches against financial institutions from 2010 to 2018

Countries	Data Theft	Thwarting customer	Total
US	1	6	7
Europe	1	2	3
Asia	3	0	3
Africa	-	-	-
Australia	1	0	1

Source: TARIQ ,NIDA (2018) IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS, Journal of Internet Banking and Commerce, vol. 23, no. 2.p2-10.

Globally, in 2021, Asian organizations experienced the largest number of breaches and attacks. The percentage of attacks on organizations by continent in 2021 was distributed as follows:: Figure (1)

Figure (1) Cyberattacks by continent in 2021



Source: ttps://aag-it.com/the-latest-cyber-crime-statistics

Second - The Financial Costs of Cyber Intrusions

The implementation of online banking has yielded numerous benefits, including reduced costs, market expansion, As service speed improves, however, there is a greater opportunity for cybercrimes and attacks., with over $3 trillion withdrawn from the system. It is noted that banking services fall victim to cybersecurity attacks at a rate 300 times higher than companies in other service sectors.

(Harrison, & Wang 2019:4)

The reported direct losses for companies may not fully cover the total economic costs of cyber incidents because companies do not report indirect losses resulting from cyber incidents—such as business loss, reputational damage, or investments in cybersecurity—due to the difficulty of monitoring these losses or the potential for them to worsen over time. (IMF, 2023:5)

Steve Morgan, founder and editor-in-chief of Cybersecurity Ventures, stated that the costs of cybercrime include the corruption and destruction of data, theft of money, loss of productivity, theft of property, theft of personal and financial data, embezzlement, fraud, disruption of normal business operations after an attack, criminal investigation, and the restoration and

deletion of breached data and systems, along with reputational harm. Cybercrime inflicts severe damage on both private and public enterprises and promotes data security and cybersecurity.

According to an investigative report by Alibaba Security's Zero Lab statistics, hundreds of thousands of telecom fraud cases occurred within China in 2017. This issue cost over 100 million yuan and involved tens of thousands of victims. Telecom fraud has remained a persistent and large-scale extortion issue up to now. (Fatma, 2020:255)

According to IBM (2024), companies suffered operational losses and financial theft, with the average global cost of a data breach rising to $4.45 million in 2023, an increase of $100,000 from 2022. This represents a 2.3% increase from the $4.35 million reported in 2022. Since 2020, when the average total cost was $3.86 million, the average total cost has increased by 15.3%.

The FBI's Internet Crime Complaint Center also reported that cybercrime caused losses of $10.3 billion in 2022, an increase from $6.9 billion in 2021. The center received 800,944 complaints in 2022, indicating a significant increase in the number of reported incidents year-on-year. (Kozier and Tyutonic, 2024:32)

Phishing is a threat faced by organizations, with average costs and losses of $4.88 in 2021. It was the most significant fraud in 2022, with an estimated 1.236 million attacks. In 2024, one in two internet user accounts in the United States was compromised. 39% of UK businesses reported experiencing a cyberattack in 2022. The average cybercrime loss for UK businesses in 2022 was £4,200. Malware attacks increased by 358% in 2020 compared to 2019.

https://aag-it.com/the-latest-cyber-crime-statistics

Table (3) illustrates the costs incurred by financial institutions as a result of cyber attacks.

Table (3) Cyber Intrusions on Financial Institutions (2010-2018)

Countries	lose money
US	4
Europe	2

Asia	6
Africa	-
Australia	0

Source :TARIQ ,NIDA (2018) IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS, Journal of Internet Banking and Commerce, vol. 23, no. 2

Annual financial losses from cybercrime in Nigeria are estimated at approximately $500 million. In terms of types of crimes, Nigeria has suffered a reputation as a haven for online fraudulent activities. This includes the infamous 419 fraud scheme, which has spread globally since the 1980s, and more recently, the "online advance fee fraud." Nigerian banks lost N159 billion to breaches between 2000 and 2013. More than half of this loss occurred in 2010, when the internet became a popular tool within banking operations, according to a 2013 report by the Nigerian Interbank Settlement System Company (NISSC) (Harrison and Wang 2019:9).

In Canada, cybersecurity reports indicate that ransomware payments have increased since 2020, partly attributed, at least likely, to the growing number of demands from large corporations. If victims choose to pay the ransom, there are no guarantees their data will be restored. According to the Canadian Anti-Fraud Centre, over 150,000 fraud reports were filed in Canada, and over $600 million was stolen since 2021.

(Communications Security Establishment, 2023:5)

Table (4) shows that all developed and developing countries were subject to attacks, with the cost to the United Kingdom amounting to $16,503,000, Germany $15,793,000, Brazil $15,783,000, Australia $15,403,000, and Japan $15,197,000. These attacks indicate that these countries enjoy high returns, which explains why these attacks are so widespread.

Table (4) The Financial Cost of Cyber Breaches

Country	Cost (thousand dollars)
UK	16502.99
Germany	15793.24
Brazil	15782.62
Australia	15403
Japan	15197.34
France	14972.28
USA	14812.12
Russia	14734.73
India	14566.12
China	13714.47

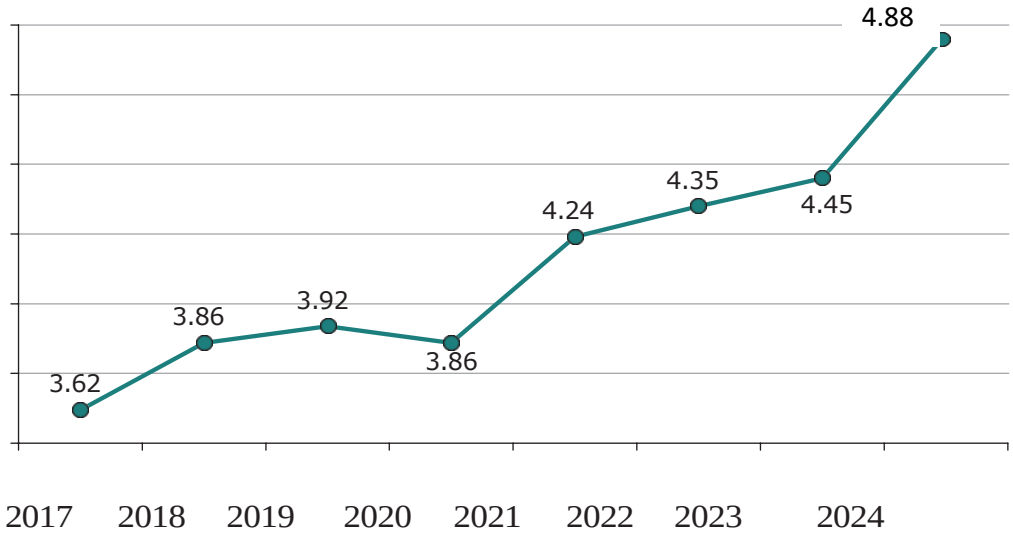
Source :Kabahing ,Sepfanner & Kartadie, Rikie(2025) Prediction of cyberattack Losses by Attack Type and Country with Visual Approach and Quantitative Statistics, Journal Software Systems, Vol.4, No.1

In one year, global banking and financial sector estimates indicate that cyberattacks cost approximately $360 billion. To address this challenge, many bankers are seeking to implement artificial intelligence (Ramadan & Hasan, 2021: 2361)

Figure (2) shows that the average data breach has increased by 10% in 2024 compared to 2023, reaching approximately $4.88 million US dollars, the highest total ever recorded. The increase in per-unit costs was particularly significant for small and medium-sized enterprises, especially since the COVID-19 pandemic. For example, for organizations with fewer than 500 employees, the cost of a data breach increased by an average of 13.4% between 2022 and 2023. However,

organizations with between 10,000 and 25,000 employees reported a decrease of 1.8%, while organizations with more than 25,000 employees experienced a 2.5% decrease during the same period.

Figure (2): Global Average Cost of a Data Breach, 2017-2024 (Million US Dollars

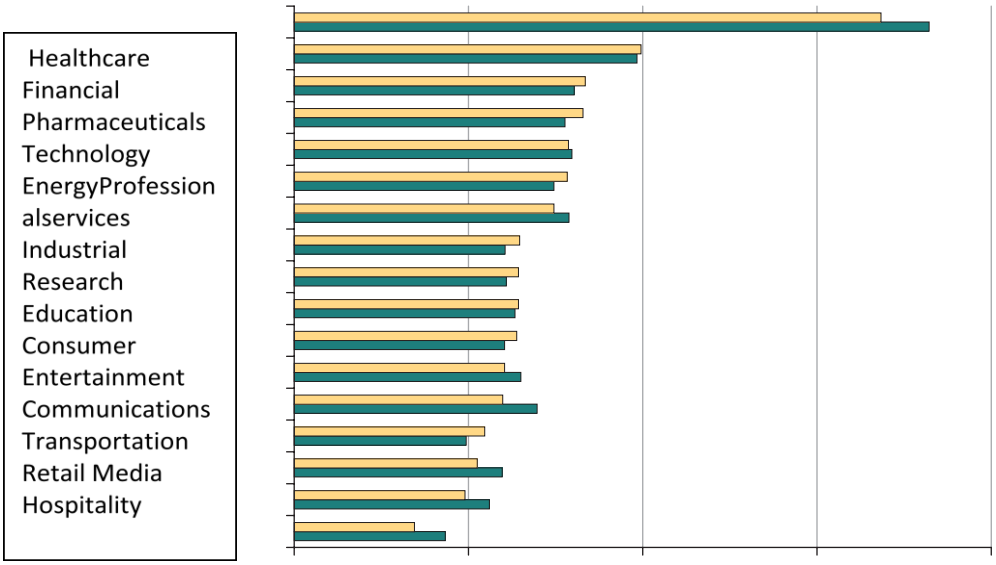


Source: Vergara, Estefania (2024) CYBERSECURIT Y ECONOMICS FOR EMERGING MARKETS, 4 International Bank for Reconstruction and Development,p54.

Across various sectors, higher data breach costs were observed in the healthcare sector, followed by the financial sectors, as shown in Figure (3). These are among the sectors most exposed to cyberattacks and breaches. These results indicate that the cost of a data breach depends on three aspects: the confidentiality of the breached data, the importance of the services at risk of disruption, and the financial assets of the targeted victim

.

Figure (3) - Data Breach Cost by Sector (2022 and 2023) (USD Billion



Source: Vergara, Estefania (2024) CYBERSECURIT Y ECONOMICS FOR EMERGING MARKETS, 4 International Bank for Reconstruction and Development,p54.

Third: Iraq's Measures to Reduce Breaches and Cyber Attacks

After 2003, Iraq's financial sector witnessed a significant wave of private bank establishment. These banks came to possess enormous capital and began dealing with internal and external financial instruments. Laws and regulations related to cybersecurity were applied; however, there are still many challenges facing the reform of current laws, including the absence of a concept of cybercrime, poor access to technology, lack of monitoring, and the failure to specify a set age for charging someone with cybercrimes. In Iraq, as a result of these reasons, (Suleiman & Hatim, 2023:37)

Regardless of the presence of strong attacks, private Iraqi banks maintain a certain level of protection. Due to security weakness in Iraq, some participants remain hesitant to use online banking servicesThus, the impact of cyber attacks varies from one country to another, depending on the characteristics of each country, with poor countries having a broader impact.. (Alismai, Shehab, 2024:174)

Iraq witnessed a decline in 2021, falling 22 places to rank 129th globally in the cybersecurity index out of 182 countries, after having been at 107th. Regionally, Iraq ranks 17th in the Arab world, only surpassing a few Arab countries (Al-Jubouri, 2025: 9). As a result of this decline, Iraqi governing bodies took some initial steps for recovery and to maintain its national security, including the following:-

1. Cybercrime Legislation in Iraq: Iraqi laws and regulations are not updated to keep pace with constantly evolving cyber threats and technologies. The judiciary applies provisions of the Iraqi Civil Code Law No. 40 of 1951. This prevents effective investigation of cybercrimes in Iraq.

2. Restrictions: Various restrictions exist in Iraq's cybercrime legislation, hindering the effective implementation of the cybercrime law and its regulations.

3. Administrative Measures: Establishing an effective national cybersecurity strategy is crucial for dealing with cybercrimes in Iraq.

4. Updating Cybercrime Legislation: In 2020, the Iraqi Council of Representatives approved a new draft law to combat cybercrimes. This law highlights various internet crimes and stipulates penalties for them. However, the new 2020 draft anti-cybercrime law did not include important amendments, given the continuous evolution of cybercrime technology, which may hinder relevant authorities from conducting effective investigations into cybercrimes in Iraq. (Suleiman & Hatim, 2023:39)

The cybersecurity of the Central Bank of Iraq (CBI), like its counterpart central banks, faces increasing challenges due to rapid technological development and the expansion of internet use, pushing the bank to take effective actions and improve its ability to respond to cyber emergencies such as (cyber attacks, electronic fraud, phishing), major structural threats, Advanced Persistent Threats (APT), digital extremism, data leakage, privacy violation, lack of cyber awareness, and attacks leading to illegal access to data, disruption of digital operations, or destruction of information. It also aims to establish policies and controls for compliance with global standard frameworks In the field of information security and cybersecurity for the CBI and the banking sector. This goal includes several sub-objectives:

1. Improving the technical infrastructure of the CBI and developing the infrastructure of the banking sector.

2. Enhancing cybersecurity maturity and data protection.

3. Working to achieve digital transformation and technical enablement of CBI and banking sector operations.

4. Adopting a strategic direction in developing the infrastructure for the electronic payment environment.

5. Implementing FinTech projects.

6. Establishing policies and controls for compliance with global standards and frameworks in information security and cybersecurity for the CBI and the banking sector.

7. Implementing systems for detecting and responding to information security, cyber, and network threats.

8. Developing smart tools for proactive protection and enhancing capabilities for examining, analyzing, and responding to information and cybersecurity events.

The CBI worked with a specialized company to develop a unified and comprehensive electronic platform to standardize the mechanism and methodology for reports on compliance procedures and the frameworks necessary for analyzing and following up on the mechanisms, plans, and implementation procedures followed by banks and electronic payment service provider companies. To improve efficiency, performance, develop processes, and adopt global standards, the CBI adopted modern technologies for its main data centers, disaster recovery centers, and branch data centers. (Cbi, 2023:23)

The Cbi directed all Iraqi banks to adopt the Customer Security Programme (CSP) framework standards approved by the global SWIFT company before the end of 2017. The CBI clarified that this request comes within the framework of the Iraqi banking sector's commitment to applying international standards in the field of financial transfers. It emphasized the necessity of restricting internet access, separating sensitive systems from the general IT environment, and

limiting cyber attacks and security vulnerabilities. (https://cbi.iq/static/uploads/up/file - Central Bank of Iraq)

2- Cyber Breach Measures in Iraq

Cyber breach measures encompass all procedures related to the confidentiality of information and data that is processed, stored, and transmitted through electronic or similar means. Official statistics for cybercrimes began to be recorded in Iraq in 2006 due to the rapid spread of online services and operations, leading to an increase in internet crimes after 2003. Weak cybersecurity and fragile infrastructure have made Iraq strategically exposed to many countries. Iraq must establish a cybersecurity system aimed at protecting its national cyberspace. Accordingly, these measures aim to develop and implement cybersecurity capabilities to enhance and sustain the following areas: (Jaber, 2025:21 & Khayon)

1. Protecting the privacy of citizens and other data from loss, harmful modifications, and unauthorized use.

2. Enhancing the resilience of government services, systems, and infrastructure against cyber threats.

3. Ensuring government continuity during and after serious cyber incidents.

4. Protecting the security of digital services provided to citizens.

5. Coordinating responses to threats against infrastructure.

-Conclusions

1. There is no distinction between developed and developing countries in terms of breaches; they are not limited by specific geographical boundaries.

2. Financial institutions are the most targeted organizations due to their close connection to money, information, and the public. Banks, as financial institutions, involve higher cyber risks compared to other organizations. For this reason, the Central Bank of Iraq directed all Iraqi banks to adopt the user protection network standards approved by the global SWIFT company before the end of 2017.

3. The judiciary applies the provisions of Iraqi Civil Law No. 40 of 1951. In 2020, the Iraqi Council of Representatives approved a new draft law to combat cybercrimes. The 2020 law did not include significant amendments, considering the continuous development of cybercrime technology, which may hinder relevant authorities from conducting effective investigations into cybercrimes in Iraq, thus preventing effective investigation of cybercrimes in Iraq.

-Recommendations

1. In light of these challenges, it is necessary to attract more advanced technology units to meet the needs of the industrial revolution, intensify efforts to enhance and develop a comprehensive cybersecurity strategy, and improve national capabilities.

2. Adopting new and broad legislation on breaches and employing electronic technical mechanisms before they become administrative and economic

Reference

1. Abdalla ,Fatma(2020) Statistics of Cybercrime from 2016 to the First Half of 2020, International Journal of Computer Science and Network, Volume 9, Issue 5
2. Al-Jubouri, Alaa (2025) Cyber Attacks and Iraqi National Security between Confrontation and Management, Al-Bayan Center for Studies and Planning.
3. Bargavi, Manju, M.Senbagavalli , Tejashwini.K.R , Tejashvar.K.R,(2022) Data Breach – Its Effects on Industry. International Journal of Data Informatics and Intelligent computing, Vol. 1, No. 2,.
4. Central Bank of Iraq. /https://cbi.iq/static/uploads/up/file
5. Communications Security Establishment,2023
6. Fotis, Friederikos (2024) Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis, International Conference on Current and Future Trends of Information .
7. Hasan ,Mohammed Faez& Al-Ramadan, Noor Salah (2021) Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case, Social Science and Humanities Journal, Vol - 05, Issue - 08

8. Jaber ,Athraa Mohammed & Khayon ,Aliaa Hameed (2025) The Role of Cyber Threats in Shaping National Security in Iraq, IMAM JA'AFAR AL-SADIQ UNIVERSITY JOURNAL OF LEGAL STUDIES , Volume 5, Issue 1.
9. Kabahing ,Sepfanner & Kartadie, Rikie(2025) Prediction of cyberattack Losses by Attack Type and Country with Visual Approach and Quantitative Statistics, Journal of Intelligent Software Systems, Vol.4, No.1
10. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R(2024) Cybersecurity and cybercrime: Current trends and threats, . Journal of International Studies, 17(2).
11. Shehab. Rami , alismai s,Abrar, etc (2024) Assessment of Cybersecurity Risks and threats on Banking and Financial Services, Journal of Internet Services and Information Security, volume: 14, number: 3.
12. Shehab. Rami , alismai s,Abrar, etc (2024) Assessment of Cybersecurity Risks and threats on Banking and Financial Services, Journal of Internet Services and Information Security, volume: 14, number: 3.p184.
13. Suleiman, Nashwan Mohammed & Hatim ,Ahmed etc(2023) Cybercrime Laws in Iraq: Addressing Limitations for Effective Governance, International Journal of Cyber Criminology –. Vol. 17(2): 33–47
14. TARIQ ,NIDA (2018) IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS, Journal of Internet Banking and Commerce, vol. 23, no. 2.
15. TARIQ ,NIDA (2018) IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS, Journal of Internet Banking and Commerce, vol. 23, no. 2.p2-10.
16. Vergara ,Estefania& Cakir Selcen (2024) A Review of the Economic Costs of Cyber Incidents.
17. Vergara, Estefania (2024) CYBERSECURIT Y ECONOMICS FOR EMERGING MARKETS, 4 International Bank for Reconstruction and Development,p54.
18. Wang ,Victoria, Nnaji .Harrison & Jeyong Jung(2019) Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability