Publication Date: 30 October 2024
Archs Sci. (2024) Volume 74, Issue 6 Pages 98-111, Paper ID 2024614.
https://doi.org/10.62227/as/74614

The Impact of Cybersecurity Spending on the Performance in Egyptian Commercial Banks with A Field Study

Abdel-Al Mustafa Abu Al-Fadl[1,*]
[1]Professor of Accounting - Shaqra University, Kingdom of Saudi Arabia.
Corresponding authors: (e-mail: aabuelfadl@su.edu.sa).

Abstract Finding the relationship between cybersecurity spending and cyber risks is the aim of the study. as well as determining how cyber threats mediate the link between commercial banks' performance and their investment on cyber security. In order to address the study questions, the investigator employed both the deductive and the inductive methods. The field study community, which consisted of bankers employed by Egyptian commercial banks, department managers, branch managers, and deputy managers, was surveyed by the researcher to gather data. From the study population, a random sample of 220 people was chosen, and 180 valid questionnaires—or 82% of all the questionnaires—were gathered. The field study's findings demonstrated that all independent variables—the amount spent on improving cybersecurity, preventing cybercrimes, and detecting them—had a favorable effect on lowering cyber risks in commercial banks. Reducing cyber risks also improved commercial banks' non-financial and financial performance. Among Egyptian commercial banks, the impact of spending on cybercrime prevention and detection ranked highest in terms of the degree to which cybersecurity spending affects cyber risks. With an average of (4.57), Egyptian commercial banks have reduced their cyber risks. The effect of investing on cybersecurity development in lowering cyber risks in Egyptian commercial banks was ranked second, with an average of (4.54). With an average of (4.88), the impact of cyber risks on financial performance in Egyptian commercial banks ranked highest in terms of the relative relevance of the degree of influence on both financial and non-financial performance. Next, with an average of (4.53), the effect of cyber threats on non-financial performance in Egyptian commercial banks ranked second. After doing the Kruskal-Wallis Test, it was discovered that there was no difference in the perspectives of the different research sample categories.

Index Terms Cost of cyber security, return on cyber security investment, cyber- attacks, cyber security, cyber risks, financial and non-financial performance, commercial banks

I. The general framework of the research

The provision of electronic banking services, or e-banking, along with electronic hardware facilities like automated teller machines (ATMs), electronic kiosks, personal digital assistants (PDAs), electronic wallets, etc., makes banking more convenient for customers and contributes significantly to the financial growth of banks. The primary obstacle to the financial growth of e-banking is cybersecurity penetration, and banks have employed Financial institutions spend hundreds of millions of dollars a year on cybersecurity, therefore commercial cybersecurity is utilized to fight cybercrime [1], [2].

One of the contemporary methods for safeguarding data connected to Internet networks and information technology is cybersecurity. Information is shielded by cybersecurity from theft and illegal access to corporate organization systems. In this area, cybersecurity policy is regarded as one of the most innovative and modern policies since it safeguards in the context of information and communications technology, this policy satisfies the needs for information availability, trustworthiness, and secrecy. Additionally, this policy improves the output quality of information systems. Banks are required by central banks to have a cybersecurity policy, with the installation of anti-hacking tools being the most crucial component [3].

A. Research problem

The average cost of a single cyberattacks on the financial sector reached $5.72 million in 2021, according to data from International Business, and the number of cyberattacks on financial institutions is increasing fourfold annually, per a 2020 Carnegie Endowment for International Peace study. IBM and "Ponemon"Foundation, demonstrating that data security has grown to be a significant concern for the banking industry. But the majority of financial institutions haven't made any efforts to improve their cybersecurity capabilities. Even while interest in cyber dangers has grown recently, many nations still haven't taken the required precautions to guard against these attacks.

Based on information released from an IMF survey of 51 countries in 2023, the majority of developing country financial officials have not resumed issuing cybersecurity regulations or

ARCHIVES DES SCIENCES
A Multidisciplinary Journal

taken action to enforce those regulations, and 56% of central banks or supervisory authorities at the level of The global financial sector lacks a national cyber strategy, 42% of countries lack a system specifically designed to manage cybersecurity risks, 68% lack a specialized risk unit, 64% have not tested their cybersecurity or offered recommendations to improve it, 54% lack a system specifically designed to report cyber incidents, and 48% lack cybercrime regulations. %6130353 at https://www.youm7.com/story/2023/3/28.

To stop cyberattacks, banks invest a lot of money in cybersecurity. The two components of cybersecurity costs are cybersecurity development costs (DC) and prevention and detection costs (PDC). Studies have shown that a small number of studies have been conducted on the cost/expenditure of cybersecurity and the financial performance of commercial banks [4]. Researchers have reported that very few studies measure the correlation between cybersecurity cost and performance for banks [5]. Furthermore, there isn't any independent research in Egypt. The relationship between cybersecurity risk, spending, and performance in commercial banks is measured by Researcher Science.

The fast digital transformation of banking operations necessitates a rise in cybersecurity spending, which may have a negative or positive impact on bank performance. Accordingly, researchers must investigate whether this spending growth is due to strategic necessity or not. This study examines the relationship between decreasing cybersecurity risks and raising cybersecurity spending. And how can performance in commercial banks be enhanced by lowering cybersecurity risks as an intermediary variable? the following primary question can be used to define the study problem in light of AIG [6], BIS [7], Fed [8], and EU [9] What effect does cybersecurity spending have on commercial banks' performance?

To answer the main research question, the following questions can be answered:

1) What is the impact of cybersecurity spending on cyber risks and hence on performance in commercial banks? In order to answer this question, it is necessary to answer the following two sub-questions:
   - What is the impact of the costs of preventing and preventing cybercrimes on cyber risks in commercial banks?
   - What is the impact of cybersecurity development costs on cyber risks in commercial banks?
2) What is the impact of cyber risks on performance in commercial banks? In order to answer this question, it is necessary to answer the following two sub-questions:
   - What is the impact of cyber risks on the financial performance of commercial banks?
   - What is the impact of cyber risks on non-financial performance in commercial banks?

B. Research objective

The goal of the research is to identify the impact of cybersecurity spending on cyber risks, and to find the mediating effect of cyber risks in the relationship with cyber security costs and on performance in Commercial banks. This is achieved through the following objectives:

1) Know the impact of cybersecurity spending on cyber risks in commercial banks. To achieve this goal, the following two sub-goals must be achieved:
   - Knowing the impact of the costs of preventing and preventing cybercrimes on cyber risks in commercial banks.
   - Knowing the impact of cybersecurity development costs on cyber risks in commercial banks.
2) Knowing the impact of cyber risks on performance in commercial banks. To achieve this goal, the following two sub-goals must be achieved:
   - Knowing the impact of cyber risks on financial performance in commercial banks.
   - Knowing the impact of cyber risks on non-financial performance in commercial banks

C. The importance of research

The study contributes to the body of literature on the cost and expenditure of cybersecurity, which will be helpful to researchers conducting similar studies because it is the first to measure the impact of cybersecurity spending on cyber risks and performance. The research is significant for scholars because it offers up-to-date, comprehensive knowledge of the impact of cybersecurity spending on cyber risks and performance in commercial banks while using cyber risk as an intermediate variable. This research is crucial for commercial banks since it helps to clarify how cybersecurity investment impacts cyber risks and performance, and how crucial this information is for decision-making regarding.

D. Research methodology

In order to address the study problems, both the deductive and the inductive approaches were prioritized. In order to create the theoretical framework and develop research hypotheses that must be tested in order to achieve the research objectives, the researcher uses the deductive approach, which is based on observation, scientific deduction, and extrapolation of reality through previous studies available in Arab and foreign research on a subject in scientific periodicals and websites related to the subject of the research. The inductive approach is used during the field study in order to test the research hypotheses on a sample of commercial banks operating in Egypt and verify the validity or incorrectness of the research hypotheses.

E. Research plan:

To answer the research questions and achieve its objectives, the researcher organized the research as follows:

1) The general framework of the research.
2) Previous studies.
3) Theoretical framework of cybersecurity and cyberrisk.

4) The impact of cybersecurity spending on cyber risks in Commercial banks.
5) Cybersecurity spending and performance in Commercial banks while mediating cyber risks.
6) Field study.
7) Research results, recommendations and proposals for future research.

II. Previous Studies

Previous studies were divided into two types of studies: studies that dealt with cybersecurity risks and studies that dealt with the impact of cybersecurity on bank performance, and they were addressed as follows:

A. Previous studies that addressed cybersecurity risks

Abu Musa study [10] It is considered one of the leading studies in this field in the Arab region. It focused on identifying the main risks that threaten the security of electronic accounting information systems in Saudi Arabia. The most important risks were entering incorrect data, destroying the data and outputs of the accounting system, sharing the same passwords with more than one employee, introducing viruses, and logging in. the system from unauthorized persons, and transferring the outputs to persons who are not permitted to view them. It concluded that many companies suffered significant financial losses due to the penetration of their accounting information systems by internal and external parties

The 2019 study by Al-Rashidi and Al-Sayed examined how Egyptian IT sector businesses' stock prices and trading volumes were affected by the disclosure of cybersecurity concerns in financial reports, and it also made a comparison with American companies. According to the study's findings, Egyptian companies do not disclose cybersecurity risks well, which has a detrimental impact on trading volume and stock prices, as well as financial performance. Additionally, it was demonstrated that American and Egyptian businesses disclose cybersecurity concerns in somewhat different ways. It was also demonstrated that the market value of the company and stock prices were positively impacted by the disclosure of cybersecurity risk management.

The study sought to determine how the disclosure of cybersecurity risk management reports affected investors' decisions to purchase shares of companies listed on the Egyptian Exchange. It also sought to determine how certain demographic factors, such as the investor's degree of experience and scientific training, affected the relationship under investigation. In order to accomplish the research's goal, a pilot study was carried out on a sample of brokerage company stock investors and financial analysts. The study found that the cybersecurity risk management report had a positive and moral influence on the decision to invest in stocks because it gives the company's business confidence in the field of cybersecurity and protection from cyberattacks, which enables investors to assess the company's ability to maintain information security and reduce the likelihood of breaches and negative events in the future, which contributes to rationalizing investors' decisions.

Qasim and Ibrahim [11] The study dealt with the relationship between information technology (availability of information technology dimensions, human resources skills, communication networks, databases) and the efficiency of banking innovations in the branches of Syrian public banks in Latakia Governorate, and the efficiency index of banking innovations was calculated by calculating the ratio of the output index to the input index, based on the Global Innovation Index model, and to achieve this, three main hypotheses were formulated, and the researcher used the questionnaire to collect the data that was analyzed using tests. Statistics: Arithmetic mean test, T-test for one sample, bilateral correlation test, and regression loading, and the study found a good positive relationship between information technology, input index and output index, but there is a weak inverse relationship between information technology and innovation efficiency index, and therefore the resources available to the public banks under study are not invested in order to achieve the efficiency of banking work with regard to providing banking innovations and achieving productivity indicators that ensure the stability of the financial position in the banking market.

Study by Mahrous, Saleh [12] The study attempted to develop the performance of internal auditing in Saudi business organizations to confront cybersecurity risks, by using the Agile Approach as one of the modern development approaches, in addition to presenting a set of proposals explaining the method and stages of applying agile internal auditing to confront cybersecurity risks. The study concluded that no... There are significant differences between the opinions of the categories of respondents regarding the continuous increase in cybersecurity risks and its effects at the level of business organizations and at the national level, and the absence of significant differences between the opinions of the categories of respondents regarding the shortcomings of the performance of traditional internal audit in the face of cybersecurity risks.

The study aimed to propose an indicator for the disclosure of cybersecurity risks within the information disclosed in the annual reports issued by economic units. The study concluded with building an indicator for the accounting disclosure of cybersecurity risks in accordance with international requirements issued by professional bodies, foreign and Arab legislation and evidence, and what was presented by the AICPA. The SEC Guidelines and the Toronto Stock Exchange (TSX) Financial Regulatory Guidelines.

Rukban Study [13] The study aimed to identify the reality of achieving cybersecurity for administrative information systems at Imam Muhammad bin Saud Commercial University, and to uncover the obstacles that limit its achievement. The descriptive survey method was applied, and the study reached several results, including: high degree of approval of the study members with a general arithmetic average (4.14) on the reality of achieving cybersecurity for administrative information systems, with a general arithmetic average of (2.63) on the obstacles that limit the achievement of cybersecurity for administrative information systems, and also with a general arithmetic average of (3.81) on the proposals that contribute

to achieving cybersecurity for information systems. Administrative.

B. Previous studies that addressed the impact of cybersecurity on bank performance

Njogu study [14] The study attempted to measure the impact of electronic information systems on the profitability of Kenyan banks. The study concluded that there is a strong positive relationship between the speed of response to emerging changes in the banking environment and profitability indicators represented by the rate of return on assets and the rate of return on equity, and that there is a significant relationship between the ability of the information system to Providing security, safety of operations and profitability of banks. Arshid study [15] The study aimed to identify the impact of investment in information technology (investment in hardware, investment in SW software and the number of ATMs) on the performance of Saudi banks, according to performance measures, which include return on assets and return on equity The literature review of relevant studies was presented There is a positive relationship between investment in information technology with its three components and return on investment, and it has been found that there is a positive effect of investment in information technology (investment in hardware, investment in software and the number of ATMs) on improving services Increasing financial performance.

The relationship between investment in information technology and the financial performance of banks in different environments was addressed. This relationship was discussed by reviewing the most important foreign and Arab studies related to the subject, and identifying the impact of information and communications technology on the profits and risks of the banking industry in the European Union. The study concluded that there is a large and positive role. To invest in information technology to improve the performance of banks operating in Europe.

Bokhari & Manzoor study [16] The study focused on the impact of applying the ISO27001 standard (Requirements for an Effective Information Security Management System) on financial performance and improving banking reputation. The study concluded that low awareness among employees and managers represents the main obstacle to implementing effective information security risk management, as most managers prefer remedial methods rather than preventive methods. It increases the cost of damages. It also provided practical evidence confirming the improvement in the financial performance of banks using the rate of return on assets and the rate of return on equity, and it was shown that banks that implemented strong information security systems enjoyed strong financial performance and improved banking reputation.

Rashwan and Qasim Study [17] The study examined the impact of cybersecurity risk management on supporting and enhancing stability and financial inclusion in Palestinian banks, as banks realize the danger of cyber breaches on stability. The study found that there is a significant impact of cybersecurity risk management on supporting and enhancing stability and financial inclusion in Palestinian banks.

Gatzert & Schubert study [18] The study clarified the relationship of electronic risk management in American banks and insurance companies with awareness and its impact on financial performance, through the disclosure of cyber risk management information in the annual reports of large and medium-sized companies, and found that there is a positive moral relationship between electronic risk management and the value of the company as measured by Tobin Q, which has a positive effect. On financial performance.

C. Results of previous studies

Through reviewing previous studies, the following was concluded:

- The topic of cybersecurity and cybersecurity risks has received a large area of studies and research in many fields.
- Some studies relied on the theoretical analysis of previous studies, and others relied on the use of statistical analysis of a number of actual data to reach conclusions regarding both cyber risks and cyber security.
- Many studies have examined the impact of investment in information technology on performance in banks. The components of investment in information technology were ATMs, mobile banking, online banking, debit and credit cards, and others.
- The scarcity of studies that addressed the relationship of cybersecurity to cyber risks and performance in Commercial banks.
- To the researcher's knowledge, previous studies have not addressed the impact of spending on cyber security on cyber risks and performance in Commercial banks.

D. What distinguishes the current study from previous studies

From the review and analysis of previous studies, it becomes clear that they address cyber risks and the impact of cyber crimes on banks in general. Previous studies did not clarify the costs that banks must take into account when spending on cyber security to prevent or limit cyber attacks, and there are no studies that addressed the impact of spending on cyber security. On the performance of Commercial banks in light of the variable mediation of cyber risks. The research seeks to fill this research gap and open the way for researchers to address this important topic from new dimensions.

E. Research hypotheses

The research seeks to test the following hypotheses: The first main hypothesis: Spending on cybersecurity affects cyber risks in Commercial banks. The first main hypothesis is divided into two sub-hypotheses:

1) The cost of preventing and detecting cybercrimes affects cyber risks in Commercial banks.

2) The cost of developing cybersecurity affects cyber risks in Commercial banks. **The second main hypothesis** Cyber risks affect the financial and non-financial performance in Commercial banks. The second main hypothesis is divided into two sub-hypotheses:
3) Cyber risks affect the financial performance of Commercial banks.
4) Cyber risks affect non-financial performance in Commercial banks

III. Theoretical Framework of Cyber Security and Cyber Risks

The theoretical framework for both cybersecurity and cyber-risk will be addressed as follows:

A. Cybersecurity

In this part, the concept, characteristics, axes, types and benefits of cybersecurity will be discussed as follows:

1) The concept of cybersecurity

Cybersecurity is concerned with designing and applying the necessary technologies, processes, controls, and practices to protect systems, networks, programs, devices, and data from exposure to attacks, electronic threats, and viruses, and filling the gaps of direct or indirect weaknesses. This is done through a set of procedures, including conducting a deliberate experimental attack to discover the gaps and work to fix them, and designing A set of response procedures and mitigation of the effects resulting from exposure to danger, damage, or unauthorized access , where the hacker seeks to manipulate the victim's digital system and control it illegally by using advanced devices or exploiting system vulnerabilities, or the user's low technological awareness (on , and in favor of), 2022).

The concept of cyber security for accounting systems expresses the degree of protection and security for managing accounting operations by providing appropriate technologies and software to ensure the prevention of internal and external cyber penetration of data, information, systems, hardware, software and accounting processes. Protection is achieved by using the cyber shield as an effective firewall to detect... Gaps (Alqahtani, F.H. [19] Cybersecurity is the practice of securing computer systems and networks against unauthorized access, by mitigating information risks and vulnerabilities, and thus this practice has become an essential part of maintaining the safety of companies and individual users. https://cutt.us/6H4AY.

The researcher believes that cybersecurity is related to securing computer systems and networks through information and communications technology from exposure to electronic attacks, threats, and viruses, and filling gaps in direct or indirect weaknesses.

2) Characteristics of cybersecurity

There are many characteristics of cybersecurity, the most important of which are [19]:

1) Trust and mistrust: Cybersecurity treats all programs, technologies, links, etc. as untrustworthy, and thus only allows reliable ones to pass and prevents malicious ones from passing.
2) Protection from internal threats resulting from low user awareness or ignorance of information security, by alerting employees to the danger to prevent hacking, as it has been shown that the most dangerous cyber threats arise due to low employee awareness, which harms the reputation of companies.
3) Protection from external threats by building a firewall that works around the clock as an electronic filter for programs and technologies to filter external digital risks, and address vulnerabilities that a third party may exploit to control and control.
4) Achieving a comprehensive vision of the strengths, weaknesses, and potential technological gaps that affect the financial performance and economic decisions of information users, working to solve them as quickly as possible, and submitting proposals to prevent their recurrence.

3) Cybersecurity policy axes

There are many axes of cybersecurity policy, the most important of which are: (Abbas, 2010 https://2u.pw/tWkeENZ; https://2u.pw/qui5BA2).

1) Defining roles and responsibilities, including responsibility for decision -making within the company regarding cyber risk management, including emergencies and crises.
2) Information management includes data governance and classification, in addition to the security and management of information and the information and communications technology environment in the company , with the aim of protecting data during the process of preparation, transfer, isolation and destruction, and tightening the control process over all electronic and non- electronic information resources, in addition to achieving the necessary security and protection of information from access or use. Unauthorized disclosure of information resources in the organization.
3) Privacy of customer data: This policy aims to preserve information related to customers and not disclose it to third parties, as well as ensuring that the privacy of the information is not violated by other employees who have nothing to do with the information.
4) Cyber risk management, in addition to protection controls to reduce and control cyber risks, as well as continuity and disaster recovery plans.
5) Determine the mechanism for disclosing the provisions of the cybersecurity policy to concerned parties.
6) Determine the owner, the scope of application, the periodicity of review and update, the powers of review and distribution, the objectives and responsibilities, the work procedures related to them, the penalties in the

event of non- compliance, and the mechanisms for examining compliance.

4) Types of cybersecurity

There are several different types of cybersecurity, which are as follows https://2u.pw/c5zCUHL : **The first type** Network Security Most electronic attacks occur through electronic networks, so there must be a solution to this problem, and one of the best solutions is to rely on cybersecurity, as it helps protect all computer networks from attacks.

The second type Cloud Security In the recent period, there has been reliance on artificial intelligence, whether by individuals or by companies, and the goal of this is to improve the quality of work, accomplish many tasks, and enhance the work experience. It is known that the amount of data that is stored is difficult to retain. Therefore, there are many different companies working to provide the best services that help solve this problem in record time, and here are the best of those services (Google Cloud) (Microsoft Azure).

The third type application security This type is one of the types of cybersecurity, as it is known that web applications are connected to the Internet, Therefore, it may be hacked and data stolen. Here, if you ask about the importance of cybersecurity, this type helps companies protect data from any attack such as (viruses - information encryption) and others. **The Type Four** Operational Security If the data is exposed to hacking, this type helps to reach many alternative plans, so it is relied upon in largest companies and institutions.

IV. The Impact of Cybersecurity Spending on Cyber Risks in Commercial Banks

Since cybersecurity risks lead to systemic risks, financial institutions find that their spending on hardware, software, high-quality systems maintenance, and workforce training is indispensable for developing a more resilient operational infrastructure , and therefore researchers see that banks incur more fixed overhead expenses that can affect net profits [20], and in this regard, [21] analyze that assessing the intangible losses of cybersecurity failures is complex since the erosion of customer confidence in banks' ability to protect their money and confidential information has been It can lead to serious repercussions, and also in the event of cyber- attacks, some losses may be incurred due to the possibility of filing lawsuits and compensation claims by affected customers or other external parties [22], and this means that banks need to analyze Benefits, costs and losses before allocating a budget for spending in cyber technology [22], however in practice banks maintain budget allocations to acquire the necessary technology without net present value analysis [23], and thus banks often spend more is optimally required and affects profits [24], and this type of research leads to a puzzling question for bank managers when they decide whether a marginal increase in spending on cybersecurity can lead to greater proportional added value [25], [26] , and the impact of spending in cybersecurity on cyber risks in commercial banks will be addressed as follows:

A. Spending in cybersecurity

Banks and financial institutions are constantly increasing their technology expenditures to overcome increasing cyber threats that increase fixed operating costs [27]. The Deloitte report shows that banks' technology expenditures (as a proportion of total revenues) rise to 7.16%, the highest among all sectors of the global economy [28]. It therefore indicates that the global financial industry is negatively affected by both direct losses resulting from cybersecurity breaches and additional cyber overhead costs , and in general the body of literature that has been developed bears a general consensus that institutions bear an additional financial burden resulting from rampant cyber incidents that Occurring due to the rapid digitization of operations and delivery of financial services , the situation is even worse because estimating economic losses resulting from a cybersecurity breach is very complex due to the multidimensional impacts of a security breach on banks' operational risks, costs, and performance [29]–[31], which means that cybersecurity risks lead to escalation of operational risks, which in turn leads to higher operational costs to negatively impact the financial results of banks and financial institutions [22], [32]–[34].

The computer is used in cybercrimes either as a means to commit a crime, as a recording system, or as a target for the crime [35] Computers may either store data as a storage device that helps carry out a crime that their owners may not possess, such as intellectual property theft. Njoroge [5]stated that in order to protect the electronic banking system from cyber-attacks, spending must be spent on cyber security to reduce its risks. Your spending budget in cybersecurity consists of: [5]).

1) Costs of cybercrimes (PDC).
2) Cybersecurity development costs (DC). The types of spending in cybersecurity represented by costs will be discussed Prevention (prevention) and detection on Crimes Cyber and cost development Security Cyber in the next part.

B. Types of spending in cybersecurity

Cybersecurity spending consists of two types of costs: cybercrime prevention and detection costs and cybersecurity development costs, and they are addressed as follows [36]

1) Costs of prevention and detection of cybercrimes: The costs of preventing and detecting cybercrimes are defined as "the monetary equivalent of any efforts to avoid cybercrimes" [36], and include the cost of updating computers by implementing an anti-virus system, and the cost of maintaining prevention measures [37]. The cost of preventing and detecting cybercrimes includes:
   - Insurance premiums
   - The cost of IT security systems such as spam filters, firewalls, antivirus software and browser extensions to protect users.
   - The cost of data security audit evaluations.

2) Cost of developing cybersecurity: These are costs related to quality and cybersecurity maintenance and include [36]
3) The cost of analyzing and evaluating data and information security systems: The focus is on the appropriate data security infrastructure and includes the following costs: https://2u.pw/X40G5U0
   - Costs of examining security vulnerabilities. Penetration testing costs.
   - Red team testing costs.
4) The cost of developing data and information security systems.
5) The cost of training employees on data security.

The researcher believes that spending in cybersecurity contributes to reducing cybersecurity risks, which has a positive impact on the financial and non-financial performance of Commercial banks, and the decrease in investment in cybersecurity contributes to increasing cyberrisks, which in turn leads to an increase in losses paid for cyberrisks. Therefore, it is necessary to briefly expose the losses resulting from the occurrence of cyber risks, as described in the next section.

C. Losses resulting from cyber risks

Cyber risks result in two types of losses that banks bear:

1) Losses in response to cybercrime: This takes into account direct losses incurred by individuals and businesses (including costs of business continuity and disaster response and recovery), as well as the costs of paying compensation to victims of identity theft, regulatory fines from industry bodies, and indirect costs associated with legal or forensic matters, including the cost of responding to crimes. Cyber include [36], [37]
   - Payment of compensation.
   - Regulatory fines.
   - Legal costs.
2) Indirect losses: These include [29], [36]
   - Damage to reputation
   - Loss of customer confidence
   - Decrease in citizens' use of electronic services as a result of decreased confidence in online transactions
   - Efforts to clean computers infected for the robot network.

D. The volume of spending in cybersecurity

There are many factors that should be taken into consideration when determining the amount of spending in cybersecurity, including https://2u.pw/5M3ZhTz:

1) The myth that all assets in the bank are protected in the same way A strong cybersecurity strategy should provide differentiated protection for a bank's most important assets, using a tiered set of security measures. Business and cybersecurity leaders must work together to identify and protect the "crown jewels" of banks that generate the most value for the bank.
2) The Myth: The more we spend, the safer we become Some banks spend a significant amount on cybersecurity and actually underperform the rest of the market when it comes to developing digital resilience, partly because they are not protecting the right assets with a comprehensive approach (protecting all assets rather than protecting the crown jewels).
3) The myth that external hackers are the only threat to a bank's assets There are significant threats from within the bank itself, and people closest to data or other bank assets are often a weak link in a bank's cybersecurity program, especially when they share passwords or files across unprotected networks or behave in other ways that open a bank's networks to attack.
4) The Myth: The more advanced our technology is, the safer we are It is true that cybersecurity groups often use powerful and sophisticated techniques to protect a bank's data and assets, but it is also true that many threats can be mitigated using less advanced methods. According to research, more than 70% of global cyberattacks come from financially motivated criminals using methods... Technically simple, like phishing emails https://2u.pw/5M3ZhTz.

E. How do we manage the amount of spending on cybersecurity in commercial banks?

Technology professionals have a role to play in re-educating senior banking officers on best practices in cybersecurity spending, specifically explaining why a tiered approach to cybersecurity is more effective than blanket coverage. A budget cannot grow or shrink depending on whether The bank has recently been exposed to breaches in the banking system, so the following must be taken into account https://2u.pw/5M3ZhTz:

- Cybersecurity spending should be considered permanent capital spending.
- Allocation priorities should be determined on the basis of a review of the full range of ongoing initiatives.
- Business and technology professionals must work together to manage the trade-offs associated with cybersecurity.

The cybersecurity team can engage executives in discussions about the most critical data assets associated with each part of the business value chain, the systems within them, the controls in place, and the trade-offs associated with protecting higher-priority versus lower-priority assets.

On a broader level, technology professionals can help senior bank officials set standards for cybersecurity spending in banks and on cybersecurity initiatives that can be reviewed regularly, and to have a comprehensive planning and review process for cybersecurity spending in banks. https://2u.pw/5M3ZhTz

ARCHIVES DES SCIENCES
A Multidisciplinary Journal

F. The role of cybersecurity spending in reducing cyber risks

The International Monetary Fund estimates annual losses at 97 billion, which represents about 9% of global banks' net profits in 2018 [38], so banks are constantly increasing their technology expenditures to overcome increasing cyber threats that increase operating costs [27], and a Deloitte report shows that banks' technology expenditures (as a share of total revenues) rise to 7.16%, the highest among all sectors of the global economy [28].

Banks need to spend sufficiently on cybersecurity to reduce cyber risks by building a flexible online technological infrastructure as recommended by international organizations. Spending is mostly in areas such as acquiring the most reliable hardware and software, data encryption systems, and firewalls. Cyber monitoring, risk detection systems, and IT training. [39], in other words, increasing spending on cybersecurity contributes to reducing cybersecurity risks as an intermediary variable, and decreasing cybersecurity risks improves financial and non-financial performance in banks. [22], [32], [34].

V. Spending on Cybersecurity and Performance in Commercial Banks in Light of the Mediation of Cyber Risks

The relationship between cybersecurity spending, cyber risks and performance in Commercial banks will be addressed as follows:

A. The impact of cybersecurity spending on cyber risks in commercial banks

Banks must maintain a high level of cybersecurity and put in place preventive measures to confront potential cyberattacks, design and implement cyberdefense programs and mechanisms to maintain the safety and security of data and people, and then stabilize banks by conducting a review of the cybersecurity system [40]. In order to reduce cyber risks, the researcher believes it is necessary for banks to achieve cyber security through spending on it, which entails two types of costs: the costs of preventing and detecting cyber crimes and the costs of developing cyber security, as spending on cyber security results in reducing cyber security risks.

B. The impact of reducing cyber risks on performance in commercial banks:

Reducing cyber risks reduces the losses resulting from the occurrence of cyber risks in Commercial banks, which are as follows:

- Losses in response to cybercrimes: which include (payment of compensation, regulatory fines, legal costs [36], [37].
- Indirect losses: which include (damage to reputation, loss of customer confidence, a decrease in citizens' use of electronic services as a result of a decrease in confidence in online transactions, efforts made to clean computers infected with malware of a botnet that sends spam [29], [36].

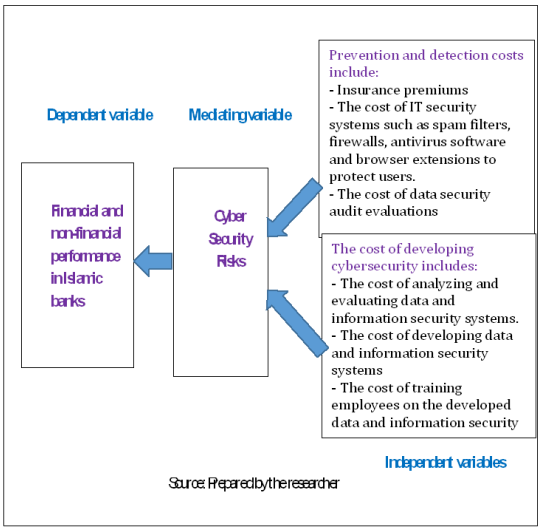

Figure 1: Spending on cybersecurity and performance in Commercial banks, with cyber risks being an intermediary variable

There is no doubt that reducing losses in response to cybercrimes leads to improving the financial performance of Commercial banks, while reducing indirect losses leads to improving the non-financial performance of Commercial banks, and this in itself calls on banks to increase spending on cybersecurity in advanced ways to mitigate the possibilities of security risks occurring. Cyber, and then improve the performance of banks.

In order to link spending on cybersecurity and performance in Commercial banks in light of cyber risk, the research variables will be presented in the next section.

C. Research variables

The researcher aims to determine whether the independent variables (the cost of prevention and detection, the cost of developing cybersecurity) have an impact on cybersecurity risks and financial and non-financial performance in Commercial banks, taking cybersecurity risks as an intermediary variable between spending on cybersecurity and performance in Commercial banks. It is shown in Figure (1) below:

Figure 1 shows that spending on cybersecurity consists of: the costs of prevention and detection of cybercrimes, and the costs of developing cybersecurity. These costs represent the independent variables that have a direct impact on the dependent variable, which is cybersecurity risks. Also, the risks Cybersecurity is an intermediary variable that affects financial and non-financial performance in Commercial banks, and spending on cybersecurity contributes to reducing cybersecurity risks, which in turn contributes to improving financial and non-financial performance in Commercial banks, which is what the field study seeks to test its validity.

ARCHIVES DES SCIENCES
A Multidisciplinary Journal

D. Summary of the theoretical study

The theoretical study concluded that increased spending in cybersecurity represented by hardware and software products designed to prevent cybercrime, anti-virus and phishing, malware infections, or unauthorized access to email accounts, as well as security measures in mitigating those risks (cost Purchasing and implementing cybersecurity technology), insurance costs and costs associated with compliance with information technology standards required for protection programs against hacking lead to reducing cyber risks. On the other hand, the study concluded that reducing cyber risks leads to improving performance in Commercial banks, whether financial performance or non-financial performance.

In the next section, the study variables are tested in the field on Saudi Commercial banks.

There is no doubt that the losses will be reduced Response For crimes Cyber technology leads to improving the financial performance of commercial banks, while reducing losses not Directly leads to improving the non-financial performance of commercial banks, And where that the average Growing continuously To change Technology Lead to more Activities Crimes e in sector Financial, and this is in Limit same He calls Banks to Increase spending in Security Cyber In ways Sophisticated To relieve from the odds happening Risks Security cyber, And from then to improve performance Banks .

In order to link spending in cybersecurity and performance in commercial banks in light of the mediation of cyber risks, the following part will present the research variables, which are spending in cybersecurity, cyber risks, and performance in commercial banks, which the research seeks to test to what extent they are valid or not.

VI. Field study

The field study aims to test the main research hypotheses, which are:

- The extent of the impact of cybersecurity spending on cyber risks in Commercial banks.
- The extent to which cyber risks affect the financial and non-financial performance of Commercial banks.

These main hypotheses were tested by testing a group of sub-hypotheses, each of which represents one of the sub-research variables, and finding field evidence that supports or rejects these hypotheses.

A. Statistical methods

The following statistical methods were used in this research:

1) Descriptive statistical measurement based on statistical packages (SPSS) to describe the characteristics of the research sample and obtain arithmetic averages and standard deviations. The hypothetical arithmetic mean of (3) was relied upon as a standard for measuring and evaluating the score obtained by the respondents.
2) Kolmogorov-Smirnov test
3) Kruskal-Wallis Test to test the significance of differences between the means of the categories of respondents.
4) One-sample T-test to compare the calculated averages with the average tabular values applied to test the research hypotheses.

B. Statistical hypotheses for the research

The first main hypothesis: There is no statistically significant effect of spending on cybersecurity on cyber risks in Commercial banks. To test this hypothesis, it is necessary to test the following two sub-hypotheses:

1) There is no statistically significant effect of the cost of developing cybersecurity on cyber risks in Saudi Commercial banks.
2) There is no statistically significant effect of spending in cybersecurity on cyber risks in Saudi Commercial banks.

The second main hypothesis: There is no statistically significant effect of cyber risks on performance in Saudi Commercial banks. To test this hypothesis, it is necessary to test the following two sub-hypotheses:

1) There is no statistically significant impact of cyber risks on the financial performance of Saudi Commercial banks.
2) There is no statistically significant impact of cyber risks on non-financial performance in Saudi Commercial banks.

The third hypothesis: There are no fundamental differences between the respondents' opinions about the impact of cybersecurity spending on cyber risks and financial and non-financial performance in Commercial banks.

C. Population and sample of the study

Due to their availability, diversity of experiences, and level of awareness, managers and deputy branch managers, department managers, and bankers employed by Egyptian commercial banks make up the field study community. A random sample of 220 people was selected from the study population, and of the total number of questionnaires, (180) correctly completed ones were collected by (82%) of the respondents, which is a good percentage for conducting statistical analysis. Table No. (2) shows the distribution of survey forms received from the study sample based on the sample categories, which were as follows:

D. Search tool

The data collection was based on a survey form that took into account simplicity, clarity, and ease of understanding in its preparation. It was reviewed by a group of arbitrators specialized in accounting at universities until it was finalized. A five-point Likert scale was used, and it was divided into two parts as follows:

- The first part: It consists of demographic data for the research sample and consists of three paragraphs.

ARCHIVES DES SCIENCES
A Multidisciplinary Journal

variable	Statement	the number	percentage
Qualification	Bachelor's	140	%77.8
	Master's	34	%18.9
	Ph.D	6	%3.3
	the total	180	%100
Job title	Branch Manager	34	%18.9
	Deputy Branch Manager	40	%22.2
	Head of the Department	44	%24.4
	banking	62	%34.5
	the total	180	%100
Years of Experience	From 5 – 10 years	66	%36.7
	15-10years	54	%30
	20-15years	34	%18.9
	Older than 20 years	26	%14.4
	Total	180	%100

Table 1: Distribution of survey forms received from the study sample According to sample categories

- Part Two: It deals with the impact of cybersecurity spending on cyber risks and financial and non-financial performance in Egyptian commercial banks. The reliability of the questionnaire was according to Cronbach's alpha ,(0.88) which is an excellent percentage as it is higher than the acceptable percentage .(%60) This means that there is a large degree of credibility in the answers to the questions.

E. Testing the statistical hypotheses for the field study

The statistical hypotheses of the field study were tested as follows:

1) The first hypothesis: There is no statistically significant effect of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Commercial banks. Table No. (3) shows the results of the impact of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Commercial banks through the arithmetic mean, standard deviation, one-sample T-test, Kolmogorov-Smirnov test, and relative importance.
   It was shown from Table No. (3) that the value of the arithmetic mean of the impact of the cost of preventing and detecting cybercrimes on cyber risks in Egyptian commercial banks was (4.57), compared to the hypothetical arithmetic mean of (3) as a standard for measuring and evaluating the score obtained, as well as the results of the sample T test. One and the results of the Kolmogorov- Smirnov test, which indicate that there are no fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted, which is: There is a statistically significant effect of the cost of preventing and detecting cybercrimes on cyber risks in Egyptian commercial banks.
2) The second hypothesis: There is no statistically significant impact of Tech Life 's cybersecurity development on cyber risks in Egyptian commercial banks.

Table No. (4) shows the results of the impact of cybersecurity development costs on cyber risks in Egyptian commercial banks, through the arithmetic mean, standard deviation, one-sample T- test, and relative importance.

It was shown from Table No. (4) that the value of the arithmetic mean for the extent of the results of the impact of cybersecurity development costs on cyber risks in Egyptian commercial banks amounted to (4.54), compared to the hypothetical arithmetic mean of (3) as a standard for measuring and evaluating the degree obtained, as well as the results of the T- test for the sample. One and the results of the Kolmogorov-Smirnov test, which indicate that there are no fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted, which is: There is a statistically significant effect of the costs of developing cybersecurity on cyber risks in Egyptian commercial banks.

1) The third hypothesis: There is no statistically significant effect of cybersecurity spending on cyber risks in commercial banks.
   Tables No. (3) and No. (4) show us the results of the extent to which cybersecurity spending affects cyber risks in commercial banks, through the arithmetic mean, standard deviation, one-sample T- test, and relative importance.
   It was shown from Table No. (5) that the value of the arithmetic mean of the extent to which spending in cybersecurity affects cyber risks in commercial banks amounted to (4.55), compared to the hypothesized arithmetic mean of (3) as a standard for measuring and evaluating the degree obtained, as well as the results of the one-sample T- test and the results of Kolmogorov-Smirnov test, which indicates that there are no significant differences between the sample items. The null hypothesis was rejected and the alternative hypothesis was accepted, which is: There is a statistically significant effect of spending in cybersecurity on cyber risks in Egyptian commercial banks.
2) Fourth hypothesis: There is no statistically significant effect of cyber risks on the financial performance of Egyptian commercial banks.
   Table No. (6) shows the results of the extent to which cyber risks affect the financial performance of Egyptian commercial banks Through the arithmetic mean, standard deviation, one-sample T- test, and relative importance.
   shows that the value of the arithmetic mean of the extent of the impact of cyber risks on financial performance in Egyptian commercial banks It reached (4.88) and compared to the hypothesized arithmetic mean of (3) as a criterion for measuring and evaluating the obtained score, as well as the results of the one-sample T- test and the results of the Kolmogorov-Smirnov test, which indicate that there are no fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted, which is: There are A statistically significant impact of cyber risks on financial performance in Egyptian commercial banks.
3) Fifth hypothesis: There is no statistically significant

ARCHIVES DES SCIENCES
A Multidisciplinary Journal

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
The costs of IT security systems such as spam filters, firewalls, anti-virus software and browser extensions to protect users contribute to reducing cyber risks in commercial banks.	4.75	0.11	0.97	21.32	0.94	0.00
Cybersecurity insurance costs contribute to reducing cyber risks in commercial banks.	4.32	0.15	0.91	21.32	0.94	0.00
The costs associated with compliance with required IT standards contribute to reducing cyber risks in commercial banks.	4.55	013	0.94	21.32	0.94	0.00
Maintenance costs and cybersecurity preventive measures contribute to reducing cyber risks in commercial banks.	4.67	0.12	0.95	21.32	0.94	0.00
Average	4.57	3 0.1	0.94	21.32	0.94	0.00

Table 2: Results of the impact of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Commercial banks

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculate d T value	Kolmogorov - Smirnov	Significant level
Vulnerability scanning costs contribute to reducing cyber risks in commercial banks	4.64	0.10	0.94	21.32	0.94	0.00
Penetration testing costs contribute to reducing cyber risks in commercial banks	4.51	0.16	0.89	21.32	0.94	0.00
The costs of data security audits contribute to reducing cyber risks in commercial banks .	4.46	0.14	0.88	21.32	0.94	0.00
The costs of providing employees with the modern knowledge and skills necessary to prevent data breaches contribute to reducing cyber risks in commercial banks	4.52	0.12	0.90	21.32	0.94	0.00
Average	3 4.5	0.13	0.90	21.32	0.94	0.00

Table 3: Results of the impact of cybersecurity development costs on cyber risks in Egyptian commercial banks.

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
Average results of how the cost of preventing and detecting cybercrimes affects cyber risks In Egyptian commercial banks	4.57	3 0.1	0.94	21.32	0.94	0.00
Average results of the impact of cybersecurity development costs on cyber risks In Egyptian commercial banks.	4.54	0.13	0.90	21.32	0.94	0.00
Average	5 4.5	0.13	2 0.9	21.32	0.94	0.00

Table 4: Results of the impact of cybersecurity spending on cyber risks in Egyptian commercial banks

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculate d T value	Kolmogorov - Smirnov	Significant level
Reducing cybersecurity risks contributes to increasing the market value of the bank's shares	4.62	0.10	0.93	21.32	0.94	0.00
Reducing cybersecurity risks contributes to reducing the amount of compensation paid	4.38	0.17	0.90	21.32	0.94	0.00
Reducing cybersecurity risks contributes to reducing the value of regulatory fines	4.43	0.15	0.89	21.32	0.94	0.00
Reducing cybersecurity risks reduces legal costs	4.51	0.11	0.92	21.32	0.94	0.00
Reducing cybersecurity risks reduces disaster response costs.	4.53	0.11	0.9	21.32	0.94	0.00
Reducing cybersecurity risks contributes to reducing business continuity costs.	4.31	0.16	0.84	21.32	0.94	0.00
Reducing cybersecurity risks contributes to increasing the bank's profitability.	4.68	0.09	0.89	21.32	0.94	0.00
Reducing cybersecurity risks contributes to increasing the rate of return on investment in the bank.	4.72	0.08	0.95	21.32	0.94	0.00
Reducing cybersecurity risks contributes to increasing the bank's rate of return on equity	7.76	0.07	0.96	21.32	0.94	0.00
Average	4.88	1 0.1	0.91	21.32	0.94	0.00

Table 5: Results of the impact of cyber risks on financial performance In Egyptian commercial banks.

effect of cyber risks on non-financial performance in Egyptian commercial banks. To measure the extent of the impact of cyber risks on non-financial performance in Egyptian commercial banks, the general arithmetic mean, standard deviation, relative importance, and one-sample T- test were calculated for the sample under study and application, and the results were as shown in Table No. (7).

Table No. (7) shows that the value of the general arithmetic mean for the range of results of the extent of the impact of cyber risks on non-financial performance amounted to (4.78), compared to the hypothetical arithmetic mean of (3) as a criterion for measuring and evaluating the obtained score, as well as the results of the one-sample T-test and the results of the Kolmogorov test. - Smirnov, which indicates that there are no fundamental differences between the sample items. The null hypothesis was rejected and the alternative hypothesis was accepted, which is: There is a statistically significant effect of cyber risks on non-financial performance in Egyptian Commercial Banks .

4) The sixth assumption: There is no statistically significant impact of cyber risks on financial and non-financial performance in Egyptian commercial banks.

Tables No. (6) and No. (7) show the results of the extent to which cybersecurity spending affects cyber risks in commercial banks, through the arithmetic mean, standard deviation, one-sample T- test, and relative importance.

It was shown from Table No. (8) that the value of the arithmetic mean of the extent to which cyber risks affect financial and non-financial performance in Egyptian commercial banks reached (4.71), compared to the hypothetical arithmetic mean of (3) as a standard for measuring and evaluating the score obtained, as well as the results of the T- test for the sample. One and the results of the Kolmogorov-Smirnov test, which indicate that there are no fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted, which is: There is a statistically significant effect of cyber risks on financial and non-financial performance in... Egyptian commercial banks.

5) There are no significant differences between the respondents' opinions about the impact of cybersecurity spending on cyber risks and financial and non-financial performance in Commercial banks.

To measure the absence of significant differences between the opinions of the respondents, the Kruskal -Wallis Test was conducted to test the significance of the differences between the means of the three categories of respondents, and the results of the test were as shown in Table No. (9).

Table No. (9) shows the results of the variance between the opinions of respondents in the four categories through the "Kruskal-Wallis Test" ,where the value of Ka^2 was (2.56), which is less than the level of significance of (3.19), and from this it is clear that there is no difference .Among the opinions of the research sample categories, the opinions of the four categories of branch managers and deputy managers, department managers, and bankers working in banks were compatible, which supports the research results. The extent of the impact of cybersecurity spending on cyber risks in

ARCHIVES DES SCIENCES
A Multidisciplinary Journal

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculate d T value	Kolmogorov - Smirnov	Significant level
Reducing cybersecurity risks contributes to enhancing customer satisfaction	4.61	0.12	0.91	21.32	0.94	0.00
Reducing cybersecurity risks contributes to enhancing employee satisfaction	4.17	0.14	0.86	21.32	0.94	0.00
Reducing cybersecurity risks contributes to improving the bank's reputation .	4.49	0.16	0.89	21.32	0.94	0.00
Reducing cybersecurity risks supports positive tracking from the bank's financial experts	4.58	0.09	0.90	21.32	0.94	0.00
Reducing cybersecurity risks contributes to attracting new customers	4.54	0.12	0.88	21.32	0.94	0.00
Reducing cybersecurity risks contributes to increasing citizens' use of electronic services.	4.69	0.09	0.84	21.32	0.94	0.00
Reducing cybersecurity risks reduces efforts to clean computers infected for the robot network.	4.62	0.11	0.92	21.32	0.94	0.00
Average	4.53	0.12	0.89	21.32	0.94	0.00

Table 6: Results of the extent of the impact of cyber risks on non-financial performance in Egyptian commercial banks

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
middle Results of the impact of cyber risks on financial performance in Egyptian commercial banks	4.88	1 0.1	0.91	21.32	0.94	0.00
middle Results of the impact of cyber risks on non-financial performance in Egyptian commercial banks	4.53	0.12	0.89	21.32	0.94	0.00
the total	4.71	0.12	0.90	21.32	0.94	0.00

Table 7: Results of the extent to which cyber risks affect financial and non-financial performance in Egyptian commercial banks.

Categories	the number	Average rank	Degrees of freedom	Ka²	Significant level
Branch Manager	35	61.1			
Deputy Branch Manager	50	56.3			
Head of the Department	60	58.7	3	2.56	3.19
banker	105	64.7			
	250				

Table 8: Results of no differences among the respondents' opinions on the impact of cybersecurity spending on cyber risks and financial and non-financial performance in commercial banks

Egyptian commercial banks can be ranked according to the degree of relative importance, as shown in Table No. (10).

Table No. (10) shows the relative importance of the degree of impact of cybersecurity spending on cyber risks in Egyptian commercial banks, as it came In first order The impact of spending on prevention and detection of cybercrimes in reducing cyber risks in Egyptian commercial banks has an average of (4.57), and in second place is the impact of spending in developing cybersecurity in reducing cyber risks in Egyptian commercial banks with an average of (4.54).

Also possible to rank the extent to which cyber risks affect financial and non-financial performance Egyptian commercial banks, according to the degree of relative importance, as shown in Table No. (11).

Table No. (11) shows the relative importance of the degree of impact of cyber risks on financial and non-financial performance in Egyptian commercial banks, In the first place was the impact of cyber risks on the financial performance in Egyptian commercial banks with an average of (4.88), and in the second place was the impact of cyber risks on non-financial performance in Egyptian commercial banks with an average of (4.53).

VII. Summary and Results of the Research and Suggestions for Future Research

A. Research summary

Spending on cyber security and cyber risks and their impact on financial and non-financial performance in Egyptian commercial banks was addressed. Cyber security risks lead to increased operational risks, which in turn lead to higher operational costs. Increasing spending on cybersecurity contributes to reducing cybersecurity risks, and cybersecurity risks, as an intermediary variable, contribute to improving financial and non-financial performance in commercial banks.

Consists of the cost of prevention and detection of cybercrimes and the cost of developing cybersecurity. Banks also bear losses resulting from increased cybersecurity risks, represented by losses in response to cybercrimes and indirect losses. There is no doubt that spending in cybersecurity It contributes to reducing cybersecurity risks, which will have a positive impact on the financial and non-financial performance of commercial banks, and the decrease in spending on cybersecurity contributes to increasing cyber risks, which in turn leads to an increase in the losses paid for cyber risks.

The relationship between investment in cybersecurity, cyber risks, and performance in commercial banks was analysed, the factors that should be taken into consideration when determining the volume of spending in cybersecurity, how to manage the volume of spending in cybersecurity in banks, and the role of the return on security investment in making the investment decision in cybersecurity.

The results of the field study showed that all independent variables (spending on preventing and detecting cybercrimes and spending on developing cybersecurity) It had a positive impact in reducing cyber risks in commercial banks. Reducing cyber risks also had a positive impact on the financial and non-financial performance of commercial banks.

B. Search results

The results of the research can be presented in the following points: In terms of measuring the extent of the impact of cybersecurity spending on cyber risks and financial and non-financial performance in Egyptian commercial banks, the results of the field study were as follows:

1) There is a statistically significant effect of the cost of preventing and detecting cybercrimes on cyber risks in Egyptian commercial banks.
2) There is a statistically significant effect of cybersecurity

ARCHIVES DES SCIENCES
A Multidisciplinary Journal

Statement	Arithmetic mean	Relative importance	Ranking of relative importance
The impact of spending on prevention and detection of cybercrimes in reducing cyber risks in commercial banks	4.57	0.94	1
The impact of spending on developing cybersecurity in reducing cyber risks in commercial banks	4.54	0.90	2

Table 9: Ranking of the extent of the impact of cybersecurity spending on cyber risks in Egyptian commercial banks

Statement	Arithmetic mean	Relative importance	Ranking of relative importance
Effect Cyber risks to financial performance in Egyptian commercial banks	4.88	0.94	1
Effect Cyber risks to financial performance in Egyptian commercial banks	4.53	0.90	2

Table 10: Ranking of the extent of the impact of cyber risks on financial and non-financial performance in Banks Commercial Egyptian.

development costs on cyber risks in Egyptian commercial banks.

3) There is a statistically significant effect of cybersecurity spending on cyber risks in Egyptian commercial banks.
4) There is a statistically significant impact of cyber risks on the financial performance of Egyptian commercial banks.
5) There is a statistically significant impact of cyber risks on non-financial performance in Egyptian commercial banks.
6) There is a statistically significant impact of cyber risks on the financial and non-financial performance of Egyptian commercial banks.
7) In terms of the relative importance of the impact of cybersecurity spending

on cyber risks in Egyptian commercial banks, the results were as follows:

- came In first order The effect of spending on prevention and detection of cybercrimes in reducing cyber risks in Egyptian commercial banks with an average of (4.57)
- It came in second place The effect of spending on developing cybersecurity in reducing cyber risks in Egyptian commercial banks has an average of (4.95).

1) In terms of the relative importance of the degree of impact of cyber risks on financial and non- financial performance in Egyptian commercial banks, the results were as follows:
    - The impact of cyber risks on the financial performance of Egyptian commercial banks came in first place, with an average of (4.88).
    - The impact of cyber risks on non-financial performance in Egyptian commercial banks came in second place, with an average of (4.53).
2) Cyber risks play an important role as an intermediary variable between spending in cybersecurity and performance in commercial banks, as it leads to... Spending on cybersecurity reduces cyber risks, which in turn contributes to improving the financial and non-financial performance of commercial banks.
3) The Kruskal-Wallis Test was conducted and it was found that there was no difference between the opinions of the categories of the research sample, and therefore the opinions of the four categories of branch managers and deputy managers, department managers and bankers working in the banks were compatible opinions, which supports the results of the research.

C. Proposals for future research

Based on the results of the research and through what was learned from previous studies, a group of future research can be proposed, for example, as follows:

1) Do more Studies on areas of spending in cybersecurity.
2) Conduct further studies on cyber risk areas in commercial banks.
3) The impact of cybersecurity spending on the strategic performance of non-financial institutions.
4) Conduct an applied study to calculate the return on security investment in financial institutions and business companies.
5) The impact of companies' disclosure of the cybersecurity risk management report on the return on security investment.

References

[1] Columbus, L. (2020). Top 10 Cyber Security companies to watch in 2020 https://www.forbes.com/sites/louiscolumbus/2020/01/26/top-10-CyberSecurity-companies-to-watch-in2020/\#3d820fd24fe6
[2] Khalil, K. (2020). Effect of cyber security costs on performance of e-banking in Pakistan. *Journal of Managerial Sciences, 14*(4), 85-99.
[3] Al-Baghdadi, Marwa Fathi Al Sayed, (2021), Economics Security Cyber in sector banker, magazine Research Legal and economic, college Rights, university Mansoura, (76):.1513-1466
[4] Desta, Y. (2018). Customers'e-banking adoption in Ethiopia (Doctoral dissertation, PhD Dissertation, Addis Ababa University, Ethiopia).
[5] NJOROGE, E. W. (2018). *Effect of Cyber Crime Related Costs On Development of Financial Innovation Products and Services* (Doctoral dissertation, JKUAT-COHRED).
[6] IG. (2016, December). Is Cyber Risk Systemic? New York: American International Group. Retrieved from https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aigcyber-risk-systemic-final.pdf
[7] BIS. (2016, June). Bank for International Settlements. Retrieved from www.bis.org/cpmi/publ/d146.pdf
[8] Fed. (2017, September). Federal Reserve Policy on Payment System Risk. Washington, USA: Federal Reserve System. Electronic copy available at: https://ssrn.com/abstract=3689162
[9] EU. (2018, May). The Directive on security of network and information systems (NIS Directive).
[10] Abu Musa, Ahmed slave Peace, (2004), Importance Risks Organized the information Accounting e, study Applied on Facilities Saudi Arabia, magazine commerce and Finance, College of Commerce, university Tanta, (2): 1-54.

[11] Kassem, S., & Ibrahim, A. (2022). The role of information technology in improving the efficiency of banking innovations (A field study on public banks in Lattakia Governorate). *Tishreen University Journal-Economic and Legal Sciences Series , 44* (2), 149-168 .

[12] Mahrous , Ramadan Arif Ramadan, And Saleh , Abu Al-Hamad Mustafa, (2022), Using the agile methodology in developing internal audit performance to confront cybersecurity risks, Journal of Financial and Business Research, 23(3):491:432

[13] Al-Rukban, Al-Jawhara bint Othman bin Ali, (2023), investigation Security Cyber For systems the information Administrative in university Imam Mohammed son Saud Commercial : a study Evaluation magazine Arabic For studies Educational and social, (20) 159 - 209 retrieved from http://: search.mandumah.com/Record1353685

[14] Njogu, J. N. (2014). *The Effect Of Electronic Banking On Profitability Of Commercial Banks In Kenya* (Doctoral dissertation, University of Nairobi).

[15] Arshid, Muhammad (2017) Impact Investment in technology the information on performance Drains Saudi Arabia, the magazine Arabic Management, 37(1):.223-207

[16] Bokhari, S. A. A., & Manzoor, S. (2022). Impact of information security management system on firm financial performance: perspective of corporate reputation and branding. *American Journal of Industrial and Business Management, 12*(5), 934-954.

[17] Rashwan , Abdul Rahman Muhammad Suleiman ; And Qasim , Zainab Abdel Hafeez Ahmed, (2022), The impact of cybersecurity risk management on supporting stability and financial inclusion in banks , the first international scientific conference entitled "The impact of cybersecurity on national security during the period 20-21 December 2022, Amman Arab University in association with the Public Security Directorate, 28:1.

[18] Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance, 89*(3), 725-763.

[19] Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *Procedia Computer Science, 124*, 691-697.

[20] Kesswani, N., & Kumar, S. (2015). Maintaining Cyber Security: Implications, Costs and Returns. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 161-164, New York: Association for Computer Machinery

[21] Eling, M., & Lehmann, M. (2018). The impact of digitalization on the insurance value chain and the insurability of risks. *The Geneva papers on risk and insurance-issues and practice, 43*, 359-396.

[22] Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability. International Monetary Fund.*

[23] Gordon, L. A., & Loeb, M. P. (2002). Return on information security investments: Myths vs. realities. *Strategic finance, 84*(5), 26.

[24] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457.

[25] Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. *Information Security Technical Report, 14*(4), 186-196.

[26] Trautman, L. J., & Altenbaumer-Price, K. (2010). The board's responsibility for information technology governance. *J. Marshall J. Computer & Info. L., 28*, 313.

[27] Euromoney. (2017, August 1). Technology investments drive up banks' costs. Euromoney magazine. London.

[28] Kark, K., Shaikh, A., & Brown, C. (2017). Technology budgets: From value preservation to value creation. *Deloitte Insights. USA: Delloite Development LLC. Str*, 2.

[29] Lewis, J. A., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage.

[30] Lever, K. E., & Kifayat, K. (2020). Identifying and mitigating security risks for secure and robust NGI networks. *Sustainable Cities and Society, 59*, 102098.

[31] Peng, C., Xu, M., Xu, S., & Hu, T. (2017). Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics, 44*(14), 2534-2563.

[32] Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector.

[33] Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability, 60*, 100989.

[34] Alodhiani, AAB (2023). Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review. *Arab Journal of Humanities and Social Sciences* , (20).

[35] Padmaavathy, P. A. (2019). Cyber crimes: A threat to the banking industry. *International Journal of Management Research and Reviews, 9*(4), 1-9.

[36] Khalil, K. (2020). Effect of cyber security costs on performance of e-banking in Pakistan. *Journal of Managerial Sciences, 14*(4), 85-99.

[37] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. *The Economics Of Information Security And Privacy,* 265-300.

[38] Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

[39] Paul, J. A., & Wang, X. J. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems,* 122, 113069.

[40] Cheng, X., Hsu, C., & Wang, T. D. (2022). Talk too much? The impact of cybersecurity disclosures on investment decisions. *Communications of the Association for Information Systems, 50*(1), 26.