JPB REVIEW
INTERNATIONAL JOURNAL OF PROFESSIONAL
BUSINESS REVIEW
ISSN: 2525-3654
OPEN ACCESS

ECONOMIC OF CYBER-SECURITY AND SOCIETY DATABASES: PROTECTING THE DIGITAL ECOSYSTEM FROM CYBER-ATTACKS

Rafika Benaichouba[A], Mohsen Brahmi[B], Laadjal Adala[C]

ARTICLE INFO

Article history:

Received: April, 25th 2024

Accepted: June, 25th 2024

Keywords:

Cybersecurity;
Digital Ecosystem;
Cyberattacks;
Data Protection;
Digital Economy.

ABSTRACT

Objective: The objective of this study is to explore the role of investment in cybersecurity and the enhancement of the digital ecosystem.

Theoretical Framework: In this topic, the main concepts and theories that under in the research are presented. Therefore, the article sheds light on the importance of taking effective measures to preserve cybersecurity and promote the digital environment. The analysis focuses on three key pillars: the digital ecosystem, the economic impact of cyberattacks, and the role of investment in strengthening cybersecurity.

Method: The method of this study is data descriptive from Statista 2023 datatbases. We have relied on this method because it is suitable for analyzing available data and statistics regarding cyberthreats and their impact on the economy and society. This method has enabled us to analyze results of reports and studies regarding cybersecurity and reach the most significant challenges facing institutions in enhancing safety and digital growth.

Results and Discussion: The results obtained reveal several key findings. Most significantly, the study finds that investment in cybersecurity significantly enhances the ability to counter growing digital threats, such as electronic piracy and malware attacks.

Research Implications: The practical and theoretical implications of this research are discussed, providing insights into how the results can be applied or influence practices in the field of the cybersecurity. These implications could encompass Firms, Organizations and individuals in our digital age (AI).

Orginality/Value: The originality value of this research study suggested that the investment in cypersecurity can significantly contribute to building a sustainable economy, promoting safe practices in the digital environment, and creating new job opportunities.

Doi: https://doi.org/10.26668/businessreview/2024.v9i7.4803

ECONOMIA DA CIBERSEGURANÇA E BASES DE DADOS DA SOCIEDADE: PROTEGENDO O ECOSSISTEMA DIGITAL CONTRA ATAQUES CIBERNÉTICOS

RESUMO

Objectivo: O objectivo deste estudo é explorar o papel do investimento na cibersegurança e na melhoria do ecossistema digital.

Referencial Teórico: Neste tópico são apresentados os principais conceitos e teorias que estão na ordem do dia na investigação. Por conseguinte, o artigo esclarece a importância de tomar medidas eficazes para preservar a

[A] PhD in Economic Sciences. Faculty of Economics, Commerce and Management, Djilati Bounaama University. Bourouba, Algeria. E-mail: r.benaichouba@univ-dbkm.dz Orcid: https://orcid.org/0009-0008-7535-8708

[B] PhD in Economic Innovation. FEM, University of Sfax. Sfax, Tunisia.
E-mail: brahmi.mohsen@gmail.com Orcid: https://orcid.org/0000-0002-0995-0761

[C] Graduate in Economic Sciences. University of Continuing Education. Mesra Daira, Mostaganem Province, Algeria. E-mail: laadjal.adala@ufc.dz Orcid: https://orcid.org/0000-0002-9515-5368

cibersegurança e promover o ambiente digital. A análise centra-se em três pilares principais: o ecossistema digital, o impacto económico dos ciberataques e o papel do investimento no reforço da cibersegurança.
Método: O método deste estudo são dados descritivos das bases de dados Statista 2023. Confiámos neste método porque é adequado para analisar os dados e estatísticas disponíveis sobre as ciberameaças e o seu impacto na economia e na sociedade. Este método permitiu-nos analisar resultados de relatórios e estudos sobre cibersegurança e alcançar os desafios mais significativos que as instituições enfrentam no reforço da segurança e do crescimento digital.
Resultados e Discussão: Os resultados obtidos revelam várias conclusões importantes. Mais significativamente, o estudo conclui que o investimento em cibersegurança aumenta significativamente a capacidade de combater as crescentes ameaças digitais, como a pirataria eletrónica e os ataques de malware.
Implicações da investigação: As implicações práticas e teóricas desta investigação são discutidas, fornecendo insights sobre como os resultados podem ser aplicados ou influenciar as práticas no campo da cibersegurança. Estas implicações podem abranger empresas, organizações e indivíduos na nossa era digital (IA).
Originalidade/Valor: O valor de originalidade deste estudo sugeriu que o investimento em cibersegurança pode contribuir significativamente para a construção de uma economia sustentável, promovendo práticas seguras no ambiente digital e criando novas oportunidades de emprego.

Palavras-chave: Cibersegurança, Ecossistema Digital, Ciberataques, Proteção de Dados, Economia Digital.

ECONOMÍA DE LA CIBERSEGURIDAD Y BASES DE DATOS DE LA SOCIEDAD: PROTEGIENDO EL ECOSISTEMA DIGITAL DE LOS ATAQUES CIBERNÉTICOS

RESUMEN

Objetivo: El objetivo de este estudio es explorar el papel de la inversión en ciberseguridad y la mejora del ecosistema digital.
Marco Teórico: En este tema se presentan los principales conceptos y teorías que se abordan en la investigación. Por ello, el artículo arroja luz sobre la importancia de tomar medidas efectivas para preservar la ciberseguridad y promover el entorno digital. El análisis se centra en tres pilares clave: el ecosistema digital, el impacto económico de los ciberataques y el papel de la inversión en el fortalecimiento de la ciberseguridad.
Método: El método de este estudio es descriptivo de datos de las bases de datos de Statista 2023. Hemos confiado en este método porque es adecuado para analizar datos y estadísticas disponibles sobre las ciberamenazas y su impacto en la economía y la sociedad. Este método nos ha permitido analizar resultados de informes y estudios sobre ciberseguridad y llegar a los desafíos más importantes que enfrentan las instituciones para mejorar la seguridad y el crecimiento digital.
Resultados y Discusión: Los resultados obtenidos revelan varios hallazgos clave. Lo más significativo es que el estudio encuentra que la inversión en ciberseguridad mejora significativamente la capacidad de contrarrestar las crecientes amenazas digitales, como la piratería electrónica y los ataques de malware.
Implicaciones de la investigación: Se discuten las implicaciones prácticas y teóricas de esta investigación, proporcionando información sobre cómo los resultados pueden aplicarse o influir en las prácticas en el campo de la ciberseguridad. Estas implicaciones podrían abarcar empresas, organizaciones e individuos en nuestra era digital (IA).
Orginalidad/Valor: El valor de originalidad de este estudio de investigación sugirió que la inversión en ciberseguridad puede contribuir significativamente a construir una economía sostenible, promover prácticas seguras en el entorno digital y crear nuevas oportunidades laborales.

Palabras clave: Ciberseguridad, Ecosistema Digital, Ciberataques, Protección de Datos, Economía Digital.

1 INTRODUCTION

For more than two decades, the internet has played a significant role in global communications and technology has become increasingly integrated in the lives of people around the world. Currently, most economic, trade, cultural, social and governmental activities are being conducted in cyberspace. And that includes all levels of individuals, nongovernmental organizations, government entities and even governments. The continuous innovations and low costs have participated dramatically in the increase of accessibility and use of the internet, hence the internet today has more than three billion users around the world (Yuchong & Qinghui, 2021, p. 8176), and the number is expected to grow to reach 7.5 billion users by 2030 (Cybersecurity Ventures, 2022, p. 17).

The number of activities conducted in cyberspace has increased with the increase of the number of individuals connected to the internet, and that has been accompanied with an increase of challenges and risks threatening the sustainability of this space. These threats include cyberattacks, and the threat of wireless communications technologies. Protecting data from cyberthreats is considered one of the most significant challenges facing this industry. These threats could have devastating consequences on the economy, threaten the safety of sensitive information and jeopardize individuals' privacy, private and public institutions and even governments to risks.

This context underscores the importance of investing in cybersecurity and enhancing the ecological environment of digital businesses. Consequently, this underlines the importance of cybersecurity. With the increase in technology the spread of digital communications, the digital ecosystem of corporations and states has become more complex and interactive which requires investing in cybersecurity and allocating financial resources to enhance the cyberinfrastructure and provide training for employees and attracting cybersecurity experts and encouraging safe digital business innovations.

This article sheds the light on the importance of investing in cybersecurity and how this investment could play a decisive role in enhancing the digital ecosystem through clarifying the means of integration and the impact of each one of these two fields on building a safe and sustainable digital environment. This article also solves the issue striking the balance between enhancing cybersecurity and innovation, with the focus on challenges and opportunities facing this vital field.

The significance of this article lies in clarifying the protection of data and information in a world that is witnessing increasing cyberthreats. It also sheds light on the role of the digital ecosystem in the integration of digital components to achieve sustainable development and enhance the understanding of investing in cybersecurity on the digital ecosystem's ability to withstand challenges.

The method of this study is descriptive, and we have relied on this method because it is suitable for analyzing available data and statistics regarding cyberthreats and their impact on the economy and society. This method has enabled us to analyze results of reports and studies regarding cybersecurity and reach the most significant challenges facing institutions in enhancing safety and digital growth

2 THEORETICAL FRAMEWORK

There are numerous studies regarding the digital ecosystem, and yet many of them have not given a specific definition of this system. We rather find that some were content with shedding light on the impact of the digital ecosystem on the economic and industrial environment.

2.1 EXPLORING THE DIGITAL ECOSYSTEM AND THE INTERACTION PATTERNS IN THE DIGITAL WORLD

Among the most prominent studies was the one conducted by the global consultancy company Accenture in 2018 which suggests that digital ecosystems stretch through markets and dissolve borders of industries (Koch, Krohmer, Naab, Rost, & Trapp, 2022, p. 1). Another study conducted by Mckinsey in 2018 suggests that establishing a digital ecosystem results major transformations in the industrial landscape which indicates that these developments have an impact on the nature of these industries and changes their dynamics (Digital McKinsey Insights, 2018).

On the other hand, other studies attempted to limit the concept of the ecosystem and focused on an essential idea which is that this system is an interactive structure composed of several different digital factors, including individuals, hardware, software, and data which interact with each other to form an interactive environment contributing to the balance of the system and creating an added value. This system must be characterized by cooperation and interaction between its components while relying on digital platforms to facilitate these operations. What supports this argument is that since the middle of the first decade of the 21st century, the services provided by leading technological companies such as ebay and Meta have lead to accelerated social and economic changes. Experiences such as Uber and Airbnb are all examples of this ongoing trend (Koch et al., 2022, p. 1).

In this context, some studies adopted various concepts to the digital ecosystem from a different perspective. Some of these definitions suggested that “digital ecosystems are social and technological systems (Kapoor et al., 2021) and that this system is characterized by cooperation and interaction between its various digital components (Subramaniam et al., 2019), i.e the cooperation between the asset owner and its consumers and creating this system. This suggests that the digital ecosystem relies mainly on interaction and cooperation between the individuals or entities who own the resources and digital assets from one hand, and the individuals or entities who are benefiting from these resources on the other.

Based on the abovementioned, the digital ecosystem is supposed to rely on digital platforms which play a role in "facilitating cooperation and interaction between members" (Hein, et al., 2020), or technology facilitates this cooperation and interaction. An example of that is an e-commerce platform which enables all sellers and buyers to interact and exchange products and services conveniently. The owners of digital assets, such as companies, developers or innovators can present their products or services on these platforms, whereas consumers may benefit from them and address their needs.

This relationship between the asset owners and the consumers creates the foundation of the digital ecosystem, as cooperation and exchange is encouraged between different parties to achieve mutual benefits and create an additional value in the digital environment.

In a related context, we emphasize that understanding the digital ecosystem is very much different from traditional businesses, the digital ecosystem benefits from different layers: the physical layer (hardware), the information layer (data), the application layer (applications), and it includes the use of technology to collect data from customers, but is also means using it as a means to create new products, provide services and create new experiences for the customers.

The key difference between the two systems is that "the digital ecosystems go beyond merely having several devices or connected applications, it rather provides companies the ability to utilize these three layers simultaneously for the customers to engage with one another seamlessly through time (IMD, 2022). In general, the benefit of these layers participates in creating a dynamic digital interactive environment which enables effective transactions and interactions amongst members and enhances their abilities to achieve their goals and create new products and services.

Based on the above, the digital ecosystem is defined as a dynamic system composed of complex interactions between diverse digital factors, including individuals, hardware, data, and software. This system is considerably similar to the traditional environmental ecosystem, as the different components interact in a common environment impacting the balance and development of this system in general.

The digital ecosystem is comprised of a number of different components which interact and integrate to achieve development and sustainable growth and mutual participation in the digital*age economy. These components include: (ICTworks, 2022)

- **software and digital devices**: these components include the applications, software and hardware used to provide digital services and information;
- **data**: this includes the different data sets and information which are collected and analyzed to achieve development goals and deliver services;
- **networks and communications**: this includes the communications infrastructure and networks that enable the flow of information and data between different components and parties;
- **individuals and organizations**: this includes the people and organizations who are using and managing the software and hardware and participate in achieving the development goals;
- **regulatory and legal framework**: these components include the frameworks, laws and policies which impact the development and use of digital technologies in a development context;
- **cooperation and partnerships**: this includes cooperation and partnerships between relevant organizations and parties to achieve development goals in a better and more efficient way.

These components are impacted by technological developments, economy and culture and constantly interact and overlap with one another in the digital ecosystem. They work together to achieve specific development goals such as improving healthcare, providing education and achieving economic growth.

Digital ecosystems can be classified according to different criteria: such as the size, function, development, level of centralization, etc. by using this ecosystems classification method we can distinguish three main types: (Barykin et al., 2020, p. 9)

- **process-oriented digital ecosystems:** this type revolves around supporting and enabling creativity and innovation and venture capital projects by using specialized services and tools. For example, it could include platforms which aim at developing new ideas and encourage cooperation between companies to launch innovative products and services and investment projects. This type aims at facilitating creativity and stimulating interaction between companies and individuals;

- **resource-oriented ecosystems:** this type focuses mainly on searching for financial and nonfinancial resources necessary to execute activities of companies and achieve business projects. Platforms such as this aim at facilitating finding the necessary resources and providing them to the members of the system. For example, the platform can instruct companies to find vendors or potential partners;
- **product-oriented ecosystems:** this type focuses mainly on offering new products or services to the market. Platforms such as this aim at facilitating development, manufacturing, and joint marketing of new products among the members of the system. This type can support cooperation in all aspects of the product's life cycle, from developing the idea, to production and marketing.

This classification assists in understanding and analyzing the interactions and potential goals of each type. There is another digital ecosystem classification which is based on several descriptive criteria related to the nature and objective of these systems. The three main types are (Brush, 2023):

- **digitizer ecosystem:** such ecosystems focus on digitizing an existing product with help of business partners. This aims at providing digital service revenue without the need for high levels of administerial complexity. This type of system can add new functions to the financial systems and generate additional revenue from the digital services. This system usually includes 20 – 100 partners from five different industries;
- **platform ecosystem:** this type of digital ecosystem focuses on providing a single platform that combines the revenue flow of this usage. In addition, the data generated from this platform may be used in similar business models and services;
- **super platform ecosystem:** this type of ecosystem aims at merging several platforms under one integrated service. It is characterized by its ability to collect data from different integrated platforms which allows it to obtain a wide variety of users data. These data are converted to revenues by using several and adjacent business models.

As per the above, it is clear that these two digital ecosystem classifications focus on the same main group of three types: systems directed towards operations, systems directed towards resources, and systems directed towards products. And despite the general similarities between them, there are some differences in the main goal of each one of them. The second classification focuses on supporting innovative operations and venture capital projects, whereas the first classification focuses on searching for and obtaining necessary resources. On the other hand, the first classification focuses on launching new products to the market, whereas the second classification aims at enabling innovative operations and facilitating cooperation between companies to launch innovative products.

2.2 THE IMPACT OF CYBERATTACKS ON INFRASTRUCTURE

The increasing reliance on technology and digital work has been accompanied by an increase in cyberattacks targeting this complex ecosystem. These attacks are a new challenge in the face of digital business sustainability and the interactions between its different components.

A cyberattack can be defined as “an act that undermines the ability or functions of the information network by using a point of weakness which provides the attacker the ability to manipulate the system” (Solfa, 2022). This definition emphasizes the detrimental impact of cyberattacks on networks and systems, highlighting that such attacks rely on exploiting security weaknesses and vulnerabilities.

The International Business Machines Corporation (IBM) defines cyberattacks as “any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device” (IBM , 2023). This definition is more holistic regarding the aims of the attack and its potential impact, this reflects the great complexity of modern cyberattacks as shown by the definition that any unauthorized access to the system and data is the key feature of a cyberattack.

As per the above, the concept of a cyberattack includes intentional effort to gain unauthorized access to systems, digital data, to alter or destroy them. This includes a wide array of activities and threats over the internet. It should be noted that this concept is undergoing constant change due to technological advances and the new methods of cyberattacks and reaching harder targets and remaining there without being discovered. Despite of that, conventional cyberattacks continue to be the most common source of attacks and include the following:

Phishing attacks: One of the most common cybercrimes. Around 3.4 billion spam emails are sent every day (Kolesnikov , 2023) and represent 41% of the total cyberattacks in 2022 according to the X-Force Threat Intelligence Index published by IBM Security, (IBM Security, 2023, p. 7). Although it is not a new form of crime, it is continuously increasing. Phishing occurs when an attacker contacts the victim through a mobile phone, email, or SMS. The attacker pretends to represent a credible institution attempting to collect private and sensitive data. It is difficult for a regular person to detect a phishing attack because it is generally directed in a different and credible manner which makes it difficult for the victim to doubt the credibility of the message. Even Microsoft sent an alert to its users regarding phishing attacks (Upadhyay & Rathee, 2022, p. 94). Phishing attacks have witnessed a significant increase during Coved-19. During the quarantine period, most people believed that any information sent from their banks or official institutions would reach them as links, hence they failed in verifying the authenticity of the information.

Ransomware attack: Ransomware is a type of malware when the attacker encrypts the victims system or files and permanently blocks access to personal data, including databases, files servers (corrupting the system) and demand a ransom to restore the victim’s system (O’Brien et al., 2022, p. 2). This is the second most common type of cyberattacks in 2022 with a percentage of 17% (IBM Security, 2023, p. 6). Institutions have found 493.33 million ransomware attacks across the world in 2022 (statista, 2023). The rate of cyberattacks is expected to increase against governments, companies, consumers, and devices throughout the next five years and will reach one attack per second in 2031, compared to one in every 11 seconds in 2021 (Morgan, 2023). It is expected that the global cost of damage caused by ransomware reached USD20 billion compared to USD325 million in 2015, an increase of 57 times. And withing a decade from now the cost will reach 265 billion.

BEC or Business Email Compromise: this type of attack represents 6% of the total reported cyberattacks in 2022 (IBM Security, 2023). It is a type of scam done by email when the attacker creates an account that appears to be of a senior official in the institution and alters some identifying information of his email to appear as a person working for the same institution in order to fool its members and transfer money or sensitive information (CRS Reports, 2023, p. 3). For example, scammers send an email to the members of an institution asking them for an urgent transfer of money. Most of the times this is done under the guise of paying late bills and these bills are not authentic and the accounts where the money is transferred to belong to the scammers.

Denial-of-Service (DoS) & Distributed Denial-of-Service: two types of cyberattacks which represent 5% of all attacks (IBM Security, 2023, p. 16). The DoS attack aims at disrupting the resources of the system and preventing the system from responding to the service requests. The attack is usually conducted by using one or a small number of hacked devices. The targeted device could be unavailable to the intended user due to the disruption of the hosting service on the internet (Biju et al., 2019, p. 4850). This form of crime is easy to detect and resolve compared to the Distributed Denial-of-Service because of the large number of hacked devices being used and distributed. It is worth mentioning that Microsoft has succeeded in dealing with an average of 1435 DDoS attacks a day in 2022 (Kolesnikov , 2023).

Supply chain attacks: this type of cyberattack targets software and technology supply chains. The main objective of these attacks is to hack the operations environment that produces and distributes software and technology, such as software developers and vendors. When the supply chain attack occurs, the attackers search for a weakness in the supply chain infrastructure. That could be done through utilizing the unprotected network protocols or the server structures lacking protection or practicing unsafe programming. Once the attackers find a point of weakness, they hack the system and change the source codes and hide harmful programs in the build and update operations (Microsoft, 2023). According to a survey conducted by the Cyber Security Hub in 2022 on a sample of institutions, 36% of the participants in the survey feel that the supply chain/third party risks are considered high (Cyber Security Hub, 2022). What makes these attacks very dangerous is that these attacks work on distributing harmful programs by using a trusted identity and credible actions.

Hack and Leak: this type of attack is an unauthorized hacking of a sensitive data storage where the perpetrator steals the data. Once the attackers gain control over the sensitive data they have two options (CRS Reports, 2023, p. 4). publish the data to expose or insult the victim, or communicate with the victim and demand a ransom to avoid publishing the data.

Zero-Day: this attack exploits “the newly found security gaps that hackers can use to attack systems. The term Zero-Day refers to when the seller or developer has learned of the malfunction, which means he must fix it “immediately”. The attack occurs immediately when the hackers exploit the malfunction before the developers have a chance to fix it (kaspersky, 2023b). this attack is considered very dangerous as there is no effective means of defense against it.

Artificial Intelligence (AI) Voice-Cloning Technology: this type of cyberattacks only appeared in the past few years as “a group of attackers take advantage of Voice-Cloning Technology with the use of artificial intelligence to simulate voices of specific individuals to convince their family members or beloved to send them money. This type of scam is an updated version of the Hi Mom or Grandparent scam when the electronic perpetrator pretends to be a family member in an emergency and asks the victim to provide financial support. This type of scam has intensified in the past few years, and modern technology makes it difficult to detect (McAfee, 2023, p. 3). This type of attack can be classified as a cyberattack that aims at scamming individuals and taking advantage of social trust.

In 2022, these types of scams caused losses of up to 2.6 billion dollars in the United States (FTC, 2023) with thousands of reports about people scammed by imposters acting as their friends or family members.

Man-in-the-Middle (MitM): the attacker aims at hacking two devices in conversation attempting to reach exchanged data or information between the parties engaged in contact (CRS Reports, 2023, p. 4). These attacks are common over public Wi-Fi networks which can be easily hacked.

Other types of cyberattacks: in addition to the aforementioned cyberattacks, there are other attacks that vary in their severity, including:

- drive-by-download: this attack occurs when the computer is infected with malware by simply visiting a website when the user does not need to click anywhere to be infected;
- password attack: this target is related to obtaining the users password by using illegal means, such as guessing the password or through reaching the password database;
- SQL injection: this attack utilizes the gaps in the databases through injecting malicious SQL statements which can create, retrieve, update or even delete available data on the hacked database;
- cross-site scripting (XSS): a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites;
- eavesdropping attack: hacking data that is transmitted between two devices;
- birthday attack: this attack relies on the birthday problem in probability theory to hack information exchanged between more than one party;
- malware: installing malicious software on the user's computer through unauthorized access (Biju, Gopal, & Prakash, 2019, pp. 4850-4851). Since 2023, around 300 thousand new malwares are created every day (Kolesnikov , 2023).

These are the most popular cyberattacks currently. The motives behind these attacks and who stands behind them vary and can be narrowed down to three main categories (IBM , 2023):

- criminally motivated attackers: criminally motivated attackers attempt to achieve financial gains through stealing money or data or obstructing businesses. Cybercriminals may hack bank accounts to steal money directly or use social scam operations to fool and convince individuals to transfer them money. They may also steal data and use them to steal identities or sell them on the web or seize them for a ransom (IBM , 2023). In this regard, an investigation report in data hacking conducted by the

American company Verizon states that the main motive of cyberattacks relies heavily on financial motives as they represent 95% of violations (DBIR, 2023, p. 8);

- personally motivated attackers: personally motivated attackers, such as disgruntled current or former employees, primarily seek retribution for some perceived slight. They may take money, steal sensitive data, or disrupt a company's systems (IBM, 2023). This applies to employees facing the possibility of being laid off or the end of their contracts;
- politically motivated attackers: politically motivated attackers are usually connected to cyberwars or cyberterrorism or "hacktivists", in cyberwars, representatives of a state, usually target their enemies' government agencies or critical infrastructure (IBM, 2023). Five hundred geopolitical cyberattacks have been confirmed around the world between 2009 – 2018. The main sources of these attacks were China and Russia with a percentage of 35% of the total politically motivated attacks, including 79 confirmed attacks by China against national governments and 75 Russian attacks (Robinson, 2022).

Hactivists do not necessarily cause major harm to their targets, they rather draw attention to their causes through announcing their attacks to the public (IBM, 2023).

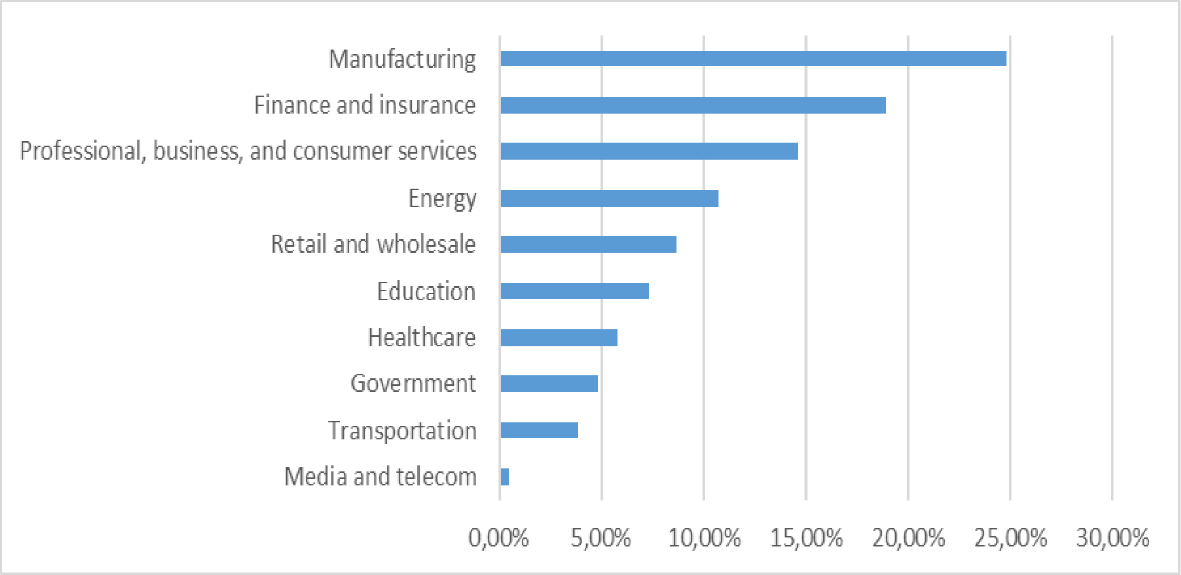
3 RESULTS AND DISCUSSSION: INVESTING IN CYBERSECURITY

Among the less common motives of cyber-hacking: commercial espionage when the attackers steal intellectual property to get an unfair advantage over their competitors. There are also vigilante hackers who take advantage of the gaps in the system to warn others.

As for the major sectors targeted by cyberattacks, it is worth mentioning that some industries are more exposed to cyberattacks than others due to the nature of their activities. And despite any industry can be exposed to data breaches, companies that play a vital role in the daily lives of individuals are usually more exposed to threats than others. Companies owning sensitive data and personal information are a common target for hackers.

Figure 1

Global Industry Landscape of Cyberattacks in 2022



Source: (Statista, 2023a)

As for the sectors most exposed to cyberattacks, Figure 1 shows that the manufacturing sector had the highest share of the total global cyberattacks in 2022. Manufacturing companies' share was 25% of the total cyberattacks followed by financing and insurance sector with 19%. Whereas professional, trade, and consumer services came in third with 14.6%.

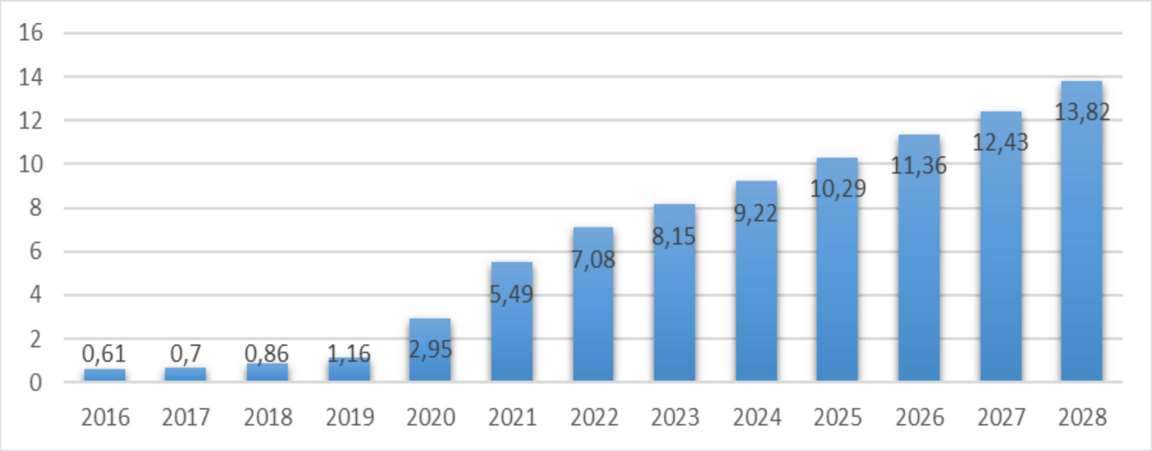
Despite that, we stress the need to mention that the size of cyberattacks targeting a specific sector is not necessarily an accurate indicator of the level of cyberthreats faced by each sector individually. In this context, Moody's credit ratings conducted a deep analysis of hacking threats for 2022 which included 71 global sectors representing assets worth 80.9 trillion dollars. The analysis showed that the sectors most exposed to hacking included hospitals and critical infrastructure such as electricity, gas, and water facilities (Moody's, 2022).

It is noticed that hospitals are a key target of cybercriminals because of the value of customers' data, especially their electronic health records (EHR) which contains sensitive information such as names of family members, social security numbers, financial details, former and current addresses, and their medical records.

We should be aware that cyberattacks and data breaches cause devastating consequences for companies, governments, and individuals. These consequences could include high costs, such as destroying data, stealing money, reducing productivity, stealing intellectual property, seizing personal and financial data, embezzlement, and scams. In addition to that, these costs include obstructing workflow after the attack, costs of criminal investigations, attempts to restore and delete the data and systems that have been hacked. We should also not forget the damage caused by the negative impact on the reputation of the attacked party.

Figure 2

Cost of Damages Caused by Cyberattacks (Trillion USD)



Source: (Statista Market Insights, 2023)

Figure 2 shows the cost of damages resulting from cyberattacks during the period from 2016-2018. It is expected that the annual global costs of damage resulting from cyberattacks will rise to reach 13.82 trillion dollars by 2028, compared with 0.61 trillion dollars in 2016. It is clear from the same figure that coved-19 and the Russia-Ukraine war had a great impact on digital businesses which lead to the increase of these attacks, hence the rise of the cost. This increase will be the biggest shift of economic wealth in history and represents a grave threat to innovation and investment motivations. This impact will be much bigger than the damage caused by natural disasters within a year, and it will be more profitable than the global trade of all illicit drugs combined.

Keeping in mind that the real cost of cyberattacks could exceed these figures dramatically as it does not include the cost incurred by the victims of ransomware including individuals and institutions and even governments that have chosen not to speak out to the authorities. Add to that the long-term effects of cyberattacks which are hard to assess.

In general, this current trend shows the significance of building robust and advanced cybersecurity strategies to address the increasing threats of digital security. These strategies must be multifaceted and based on cutting-edge technologies for the detection and protection from cyberattacks in addition to plans to deal with any security breaches actively and swiftly (Solfa, 2022, p. 20).

In brief, the increase of cyberattacks rate reflects constant challenges to the institutions working in the field of cybersecurity and makes it necessary to develop robust cyber strategies to preserve the safety of data and the reputation of institutions in a world full of digital threats

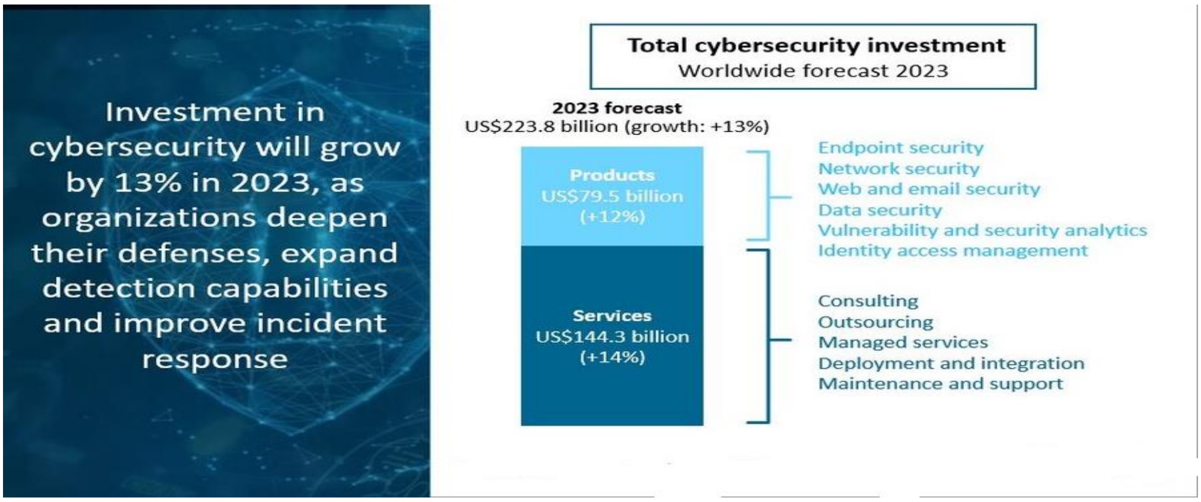
The size of investment in cybersecurity is determined by several factors, including the size and type of organization itself, the extent of security measures, and potential risks. The level of each factor directly impacts the cost of cybersecurity.

According to a survey conducted by Deloitte Insights, organizations usually allocate 10.9% of their IT budgets to cybersecurity. As for the percentage of spending of cybersecurity compared to the total income, companies allocate 0.48% of their total income to cover the costs of cybersecurity (Bernard, Golden, & Nicholson, 2020). This reflects the increasing interest in cybersecurity and its importance in protecting sensitive information and data.

As for spending on cybersecurity per employee, respondents to the survey expressed an average investment of USD2700 on each full-time employee to conduct cybersecurity (Bernard, Golden, & Nicholson, 2020). This shows the commitment of companies to train their employees and increase their awareness regarding safety.

Figure 3

Global Projected Total Investment in Cybersecurity for 2023



Source: (Canalys, 2023)

To better understand the fields of investment in cybersecurity, Figure 3 provides an overview of the expected growth of the cybersecurity sector in 2023 and how investments were distributed between diverse services and products in this sector. This graph was provided by Canalys, a firm specialized in market analysis and providing strategic outlook in technology and cybersecurity. The graph shows that investments in this sector will witness a 13% growth this year, which means that corporations will increase their investments in cybersecurity to enhance their defenses and expand their ability to detect threats and enhance their readiness to deal with potential cyber breach.

According to Figure 3, investments in cybersecurity products are expected to reach USD79.5 million in 2023, which is an increase of 12% compared to the previous year. As for expected investment in cybersecurity services in the same year, they are expected to reach USD144.3 billion, which is an increase of 14% compared to the previous year.

Overall, total investment in cybersecurity in 2023 is expected to reach USD223.8 billion, compared to 150 billion in 2021 (Aiyer, Caso, Russell, & Sorel, 2022, p. 2).

As for the industries that will witness the biggest investments in security products and services in 2023, according to a report by Worldwide Security Spending Guide, issued by International Data Corporation (IDC), these industries include banks, Discrete Manufacturing, professional services consultancies, federal/central governments (IDC, 2023). It is noticeable that banks and discrete manufacturing invest almost equally in software and services whereas professional services consultancies tend to invest largely in software, with a focus of governance, risks, compliance, and endpoint security.

In 2023, the United States is expected to be the biggest spending geography on security, lead by individual manufacturing and professional services consultancies. The second biggest geography is Western Europe and the leading sectors there are banks and discrete manufacturing. Other major geographies spending on security include Asia/Pacific, except Japan and China and of course the People's Republic of China (IDC, 2023).

In addition to the above, institutions work on enhancing security from the inside through multiple efforts. Providing qualified employees in cybersecurity is a key aspect. There is an urgent need for those professionals due to the clear global shortage in the security workforce. Shortage in security workforce reached 3.4 million by the end of 2022 (ISC2, 2022, p.7). This makes cybersecurity a lucrative field to work in, especially in North America as the average salary of cybersecurity expert reaches USD134,800. The figure drops to USD93,535 in Europe and MENA, and drops even more in Latin America to reach USD22,185 (Kerner, 2023)

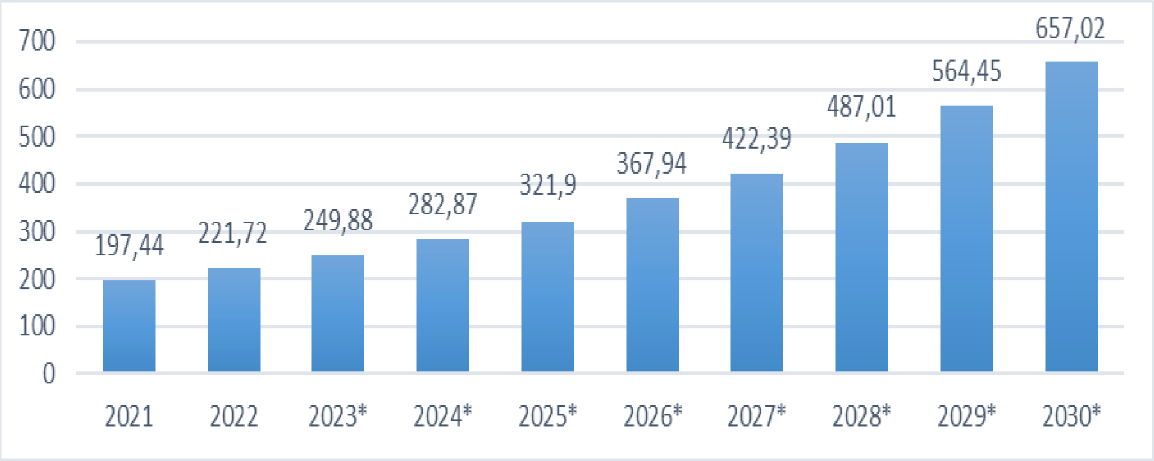
In addition to employing professionals, institutions usually utilize security awareness programs with their employees, these programs are considered a crucial part of the security strategy of any organization. Workers of all levels in the company, from regular employees to CEO's are continuously exposed to cyberattacks through phishing emails and they must be aware of the importance of security and how it could impact their daily work. This means that companies must develop training programs that aim to spread awareness amongst employees regarding the concepts and basics of cybersecurity. For example, in 2022 the programs hosted 20 events with the participation of the employees to learn about safety through simulating cyberattack scenarios (like a simulation of a potential email scam) and participating in activities to enhance communication between teams (McKinsey & Company, 2022). These programs are considered very important nowadays, specially with the difficulty to find competent and qualified employees in cybersecurity.

It is worth mentioning that regular security training for employees could participate in reducing the cost of data hacking by an average of USD232,867 (IBM Security, 2023b) because employees are usually the weakest link in the security situation of the institution and could unintentionally cause a breach of data through procedures such as clicking on phishing email or using a weak password.

In a related context, according to Figure 4, the interest in cybersecurity is expected to grow in the future. The cybersecurity market is expected to grow by 12.8% annually to reach USD657 billion in 2030 (Next Move Strategy Consulting, 2022).

Figure 4

Global Cybersecurity Market Size from 2021 to 2030 (USD Billion)



Source: (Next Move Strategy Consulting, 2022).

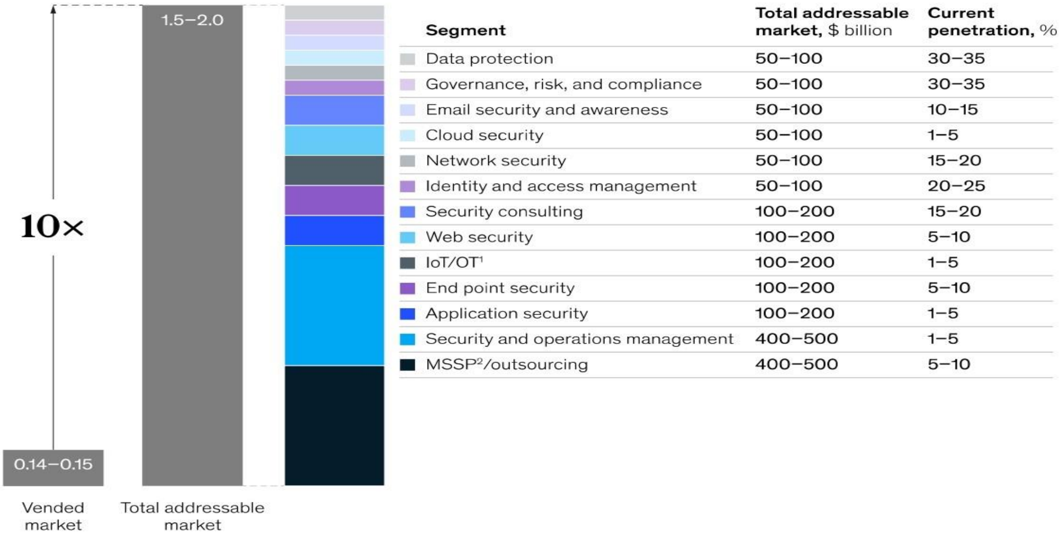
This growth is directly connected to the evolving of cyberattacks and increasing challenges facing companies in their attempts to counter them. These challenges can be summarized into three key points which are expected to have a substantial impact on institutions in the coming years:

- increase of access to data and information platforms: this trend indicates that accessing big data and information on a wide scale will increase in the future. Many technological advancements such as mobile phones and remote work rely on fast access to big data which will increase the possibility of data security breaches. Companies gather more information about customers to understand their purchasing behavior and forecast demand sufficiently. Companies are now responsible of saving and protecting this data which require state of the art technology such as data lakes which can collect data from different environments. Modern attacks benefited from this increasing access to data, points of weakness in these data are considered an opportunity for hackers;
- the growing sophistication of cyberattacks due to the use of AI and Machine Learning: hackers and attackers no longer rely on traditional attacks alone; they are using advanced technology such as AI and machine learning in their attacks. These technologies allow them to reduce the time of their attacks from weeks to hours which makes them more complicated and fatal. There is an increase in the use of technology and there is a strong indication that the use of AI makes attacks more complicated;
- the increase of regulatory pressure and the gaps in cyber resources, knowledge and skills: as we have previously mentioned, many institutions face a lack of specialized human resources and expertise in networks security. This shortage is increasing with time. Companies are also facing challenges in properly recognizing and managing digital risks as they are facing stricter regulatory demands due to the increasing concern regarding privacy and the significant breaches in cybersecurity. The result is an increase in the number of regulations related to the cross-border flow of data. These developments increase the pressure on companies to effectively determine and manage digital risks (Boehm et al., 2022).

From the above, the expected growth in the cybersecurity market will not be enough due to the size of the challenges facing institutions. There are major opportunities in the cybersecurity technology market estimated at 2 trillion dollars, given the market covers only 10% of the current market needs of security solutions (Aiyer, Caso, Russell, & Sorel, 2022, p. 2) .There is a big possibility to increase the reliance on safety networks in the future, hence increase the opportunities of the market dramatically.

Figure 5

Global Cybersecurity Market Actual Size for 2021



Segment	Total addressable market, $ billion	Current penetration, %
■ Data protection	50–100	30–35
■ Governance, risk, and compliance	50–100	30–35
■ Email security and awareness	50–100	10–15
■ Cloud security	50–100	1–5
■ Network security	50–100	15–20
■ Identity and access management	50–100	20–25
■ Security consulting	100–200	15–20
■ Web security	100–200	5–10
■ IoT/OT[1]	100–200	1–5
■ End point security	100–200	5–10
■ Application security	100–200	1–5
■ Security and operations management	400–500	1–5
■ MSSP[2]/outsourcing	400–500	5–10

Source: Aiyer et al. (2022, p. 2)

Figure 5 shows the major difference between the current size of the cybersecurity market and its size when reaching full potential which could be between 1.5 – 2 trillion dollars. This means that cybersecurity service providers are required to improve their abilities and rethink their strategies to reach customer and better respond to the demands of the categories not yet included in.

There is a great opportunity for cybersecurity service providers to benefit from this gap and take a market share with a value of 2 trillion dollars through focusing on 4 key fields:

- *cloud technologies:* cloud computing represents a tremendous development in the world of technology. Cloud computing provides great opportunities for companies and institutions to achieve success and sustainability in the market. A Mckinsey study, that included 700 Fortune 500 companies which rely on cloud computing technology, has shown that they can reach a value of over one trillion dollars by 2030 (McKinsey & Company, 2022) .Cybersecurity service providers must therefore be able to protect public and specialized cloud environments that many customers rely on;
- *pricing mechanisms:* most cyber solutions available today in the market do not target small and medium companies (McKinsey & Company, 2022) .Cybersecurity service providers must therefore target this market through creating tailored products for this market;
- *artificial intelligence AI:* there is massive potential in innovative AI and machine learning in cybersecurity. These technologies can assist in lowering the cost resulting from data breaches by 3.6 million dollars (IBM Security, 2023b). These technologies can also help

in detecting and preventing data breaches faster and more effectively than manual operations which will in return reduce the total cost resulting from data breaches. Even so, confidence in independent smart cyber defense platforms and productions remains a challenge. Therefore, cybersecurity service providers must head towards developing AI and machine learning products which will enhance the competency of human analysts and increase their ability to intervene efficiently and effectively;

- *managed services:* the demand on full services offers is expected to increase by 10% annually for the next three years (Aiyer, Caso, Russell, & Sorel, 2022). Cybersecurity service providers must develop bundled offers including important use cases. They should also focus on the results achieved by the service, not only the used technology.

In summary, cybersecurity service providers must strike a balance between products and prices and the services they can provide to respond to the demands of the targeted market, and to be agile enough to expand. If the industry was able to achieve these goals, it would definitely increase its spread and reach the two trillion-dollar threshold.

4 IMPLICATION POLICY: CYBERSECURITY TO ACHEIVE A PROPER BALANCE IN THE DIGITAL ECOSYSTEM

Cybersecurity is considered a complex concept that has been given many different definitions. We mention here the definition given by the American Department of Defense (The Pentagon) which states that it is all regulatory procedures necessary to guarantee protection of information of all kinds, physical or electronic, from different types of crimes such as attacks, vandalism, espionage, and accidents (Solfa, 2022).

The International Telecommunication Union defines cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment (ITU, 2023).

Based on the above, cybersecurity is defined as the practice of providing protection to systems, networks, and software from cyberattacks that aim to access sensitive information and change or destroy them or extort money from users or obstruct commercial businesses. Cybersecurity usually follows a multilayered protection methodology across computers, networks, software, and data. Users, operations, and technology must work together to put effective defense systems against cyberattacks.

Investing in cybersecurity is the effort, financial and human resources allocated by governments, individuals and organizations to enhance the security of their systems and digital infrastructure to face cyberthreats and attacks. This investment is necessary to achieve a proper balance in the digital ecosystem. Insufficient control over cyberattacks and security gaps will potentially lead to the collapse of the system and expose digital businesses and their components to risks.

5 CONCLUSION

Investing in cybersecurity is a decisive matter to guarantee the proper balance inside the digital ecosystem. Due to the increasing cyberthreats and continuous technological developments, institutions, governments, and individuals must invest sustainably in enhancing cybersecurity.

Institutions and governments are facing great pressure to protect their data and systems from increasing cyberthreats. Investment in cybersecurity has therefore become not an option, but a necessity. Cybersecurity enhances confidence in the use of technology and protects sensitive data and vital information. Institutions, governments, and individuals must invest sustainably in developing cyber expertise and skills and in adopting the latest technologies to counter new and continuous threats.

1. results of the study: this paper has reached several results, mainly:

- the digital ecosystem relies heavily on digital platforms that facilitate cooperation and interaction between its components. This encourages the exchange of products and services and participates in creating a dynamic digital interactive environment;
- digital ecosystems play a role in economic transformation. They can facilitate economic operation and enhance interactions between economic agents, hence enhance sustainable development and economic growth;

- with the development of technology, cyberattacks have evolved and become more complex. This requires individuals and institutions to push stronger towards cybersecurity;
- investment helps in enhancing cybersecurity and protecting sensitive data and digital assets and guaranteeing the sustainability of digital systems;
- companies around the world as a whole face challenge in qualified human resources (specialists and experts in cybersecurity) to execute cybersecurity strategies effectively;
- increase of awareness regarding cybersecurity among employees through training programs participates dramatically in reducing costs resulting from cyber threats;
- new technologies such as AI and cloud computing assist in enhancing cybersecurity's ability to counter threats effectively;
- the cybersecurity market is witnessing tremendous growth, and this provides an opportunity to service providers to invest and innovate in this field.

2. Recommendations: based on the above results, following are the recommendations:

- institutions must allocate proper resources to enhance cybersecurity, that includes increasing their budgets and employing qualified individuals and directing investments towards improving security.
- it is essential that institutions invest in state-of-the-art security technologies that deal with evolving threats. These technologies include advanced AI-powered protection systems and data analysis to detect abnormal and suspicious patterns in the behavior of the users and computer systems.
- institutions and governments must review and update their security policies regularly to guarantee their compatibility with modern threats and security legislations.
- institutions must develop awareness programs related to cybersecurity and train their employees on the concepts of security and how to counter threats
- institutions and governments exposed to cyberthreats must set incident response plans that determine the procedures that should be followed in case the system is hacked.
- cybersecurity service providers must be aware of the latest developments in these fields and set strategies focusing on those trends to guarantee responding to the demands of the clients and the maximum benefit of available technology.

REFERENCES

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers.* Récupéré sur McKinsey & Company: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers#/

Barykin, S., Kapustina, I., Kirillova, T., Yadykin, V., & Konnikov, Y. (2020). Economics of Digital Ecosystems. *Journal of Open Innovation: Technology, Market, and Complexity, 6*(4), 1-16. doi:https://doi.org/10.3390/joitmc6040124

Bernard, J., Golden, D., & Nicholson, M. (2020, July 24). *Reshaping the cybersecurity landscape , How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions*. Retrieved from Deloitte Insights: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

Biju, J., Gopal, N., & Prakash, A. (2019). CYBER ATTACKS AND ITS DIFFERENT TYPES. *International Research Journal of Engineering and Technology (IRJET), 6*(3), 4849-4852. Retrieved from https://d1wqtxts1xzle7.cloudfront.net/60557348/IRJET-V6I3124420190911-33891-1hcvf72-libre.pdf?1568195260=&response-content-disposition=inline%3B+filename%3DIRJET_CYBER_ATTACKS_AND_ITS_DIFFERENT_TY.pdf&Expires=1694345396&Signature=GQe9rg3uDBgeuF-6C4wnAmEIf

Boehm, J., Lewis, C., Li, K., Wallance, D., & Dias, D. (2022). *Cybersecurity trends: Looking over the horizon*. Retrieved March 1, 2023, from McKinsey & Company: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon#/

Brush, K. (2023). *digital ecosystem*. Retrieved August 29, 2023, from TechTarget: https://www.techtarget.com/searchcio/definition/digital-ecosystem

Canalys. (2023). *Cybersecurity investment to grow by 13% in 2023*. Retrieved from Canalys forecasts: https://www.canalys.com/newsroom/cybersecurity-forecast-2023

CRS Reports. (2023). *Cybersecurity: Selected Cyberattacks, 2012-2022.* New York: Congressional Research Service.

Cyber Security Hub. (2022). *The global state of the cyber security industry 2022, Exploring the current trends, challenges and investment opportunities within the cyber security industry*. Retrieved from https://www.cshub.com/executive-decisions/articles/cs-hub-2022-mid-year-report

Cybersecurity Ventures. (2022). *Official Cybercrime Report.* Northport, N.Y: eSentire. Retrieved from https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

DBIR. (2023). *Data Breach Investigations Report.* New Jersey: Verizon Business.

Digital McKinsey Insights. (2018, January). *Winning in digital ecosystems*. Retrieved from McKinsey & Company: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20McKinsey%20Insights%20Number%203/Digital-McKinsey-Insights-Issue-3-revised.ashx

Faris Al-Amarat and Mohammed Al Hamamsa (2022). *Cybersecurity (the concept and modern day challenges)*. Amman, Dar AlKhaleej for Press, Printing and Publishing

FTC. (2023). *New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022, Reported fraud losses increase more than 30 percent over 2021*. Retrieved September 14, 2023, from Federal Trade Commission, Protecting America's Consumers: https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

Hein, A., Schreieck, M., Riasanow, T., Setzke, D., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets, 30*(1), 87-89. doi: https://doi.org/10.1007/s12525-019-00377-4

IBM . (2023). *What is a cyberattack?* Retrieved from International Business Machines: https://www.ibm.com/topics/cyber-attack

IBM Security. (2023). *IBM Security X-Force Threat Intelligence Index 2023*. France: Compagnie IBM.

IBM Security. (2023b). *Cost of a Data Breach Report 2023*. United States of America: IBM Corporation. Retrieved from https://www.ibm.com/downloads/cas/E3G5JMBP

ICTworks. (2022, January 21). *What is Digital Ecosystem in International Development Programs?* Retrieved August 29, 2023, from ICTworks: https://www.ictworks.org/digital-ecosystem-international-development/

IDC. (2023). *New IDC Spending Guide Forecasts Worldwide Security Investments Will Grow 12.1% in 2023 to $219 Billion*. Retrieved August 14, 2023, from International Data Corporation : https://www.idc.com/getdoc.jsp?containerId=prUS50498423

IMD. (2022). *Everything you need to know about Digital Ecosystems*. Retrieved August 29, 2023, from International Institute for Management Development: https://www.imd.org/reflections/digital-ecosystems/

ISC2. (2022). *Cybersecurity Workforce Study, 2022*. Retrieved September 20, 2023, from ISC2, Inc: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196

ITU. (2023). *Definition of cybersecurity*. Retrieved from International Telecommunication Union (ITU): https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Kapoor, K., Bigdeli, A., Dwivedi, Y., Schroeder, A., Beltagui, A., & Baines, T. (2021). A socio-technical view of platform ecosystems: Systematic review and research agenda. *Journal of Business Research, 128*, 94-108. doi: https://doi.org/10.1016/j.jbusres.2021.01.060

kaspersky. (2023b). *What is a Zero-day Attack? - Definition and Explanation*. Retrieved August 26, 2023, from AO Kaspersky Lab: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Kerner, S. (2023). *34 cybersecurity statistics to lose sleep over in 2023*. Retrieved September 2, 2023, from TechTarget: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

Koch, M., Krohmer, D., Naab, M., Rost, D., & Trapp, M. (2022). A matter of definition: Criteria for digital ecosystems. *Digital Business, 2*(2), 1-13. doi: https://doi.org/10.1016/j.digbus.2022.100027

Kolesnikov , N. (2023). *50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who & What is Targeted*. Retrieved September 14, 2023, from Techopedia: https://www.techopedia.com/cybersecurity-statistics

McAfee. (2023). *Beware the Artificial Impostor: A McAfee Cybersecurity Artificial Intelligence Report.* San José, Californie, USA: McAfee, LLC. Retrieved from https://media.mcafeeassets.com/content/dam/npcld/ecommerce/en-us/resources/cybersecurity/artificial-intelligence/rp-beware-the-artificial-impostor-report.pdf

McKinsey & Company. (2022). *Building a cybersecurity culture from within: An interview with MongoDB.* Retrieved from McKinsey & Company: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/building-a-cybersecurity-culture-from-within-an-interview-with-mongodb

McKinsey & Company. (2022). *What is cloud computing?* Retrieved August 30, 2023, from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cloud-computing#/

McKinsey & Company. (2023). *What is cybersecurity?* Retrieved from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity#/

Microsoft. (2023). *Supply chain attacks*. Retrieved September 6, 2023, from Microsoft 365 documentation: https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide

Moody’s. (2022). *Industries boost cyber defenses against growing number of attacks*. Retrieved from Moody’s: https://www.moodys.com/web/en/us/about/insights/data-stories/cyber-risks-are-rising.html

Morgan, S. (2023). *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Retrieved Jul 10, 2023, from Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Next Move Strategy Consulting. (2022). *Cyber Security Market by Component (Hardware, Software, and Services), Security (Network Security, Endpoint Security, Application Security, Cloud Security, and Others) Deployment Mode (Cloud and On-Premise), Organization Size (Small & Medium-Sized Enterpr*. Retrieved September 1, 2023, from Next Move Strategy Consulting: https://www.nextmsc.com/report/cyber-security-market

O’Brien, N., Ghafur, S., Sivaramakrishnan, A., & Durkin, M. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *Digit Health, 8*, 1-3. doi: DOI: 10.1177/20552076221104665

Robinson, J. (2022). *Cyberwarfare statistics: A decade of geopolitical attacks*. Retrieved September 17, 2023, from Privacy Affairs: https://www.privacyaffairs.com/geopolitical-attacks/

Solfa, F. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. *International Journal of Technology, Innovation and Management (IJTIM), 2*(2), 18-32. doi: https://doi.org/10.54489/ijtim.v2i2.98

statista. (2023). *Annual number of ransomware attempts worldwide from 2017 to 2022*. Retrieved September 14, 2023, from statista: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/

Statista. (2023a). *Distribution of cyber attacks across worldwide industries in 2022*. Retrieved October 1, 2023, from Statista: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

Statista Market Insights. (2023). *Cybersecurity - Worldwide*. Retrieved September 20, 2023, from statista: https://www.statista.com/outlook/tmo/cybersecurity/worldwide#cybercrime

Subramaniam, M., Iyer, B., & Venkatraman, V. (2019). Competing in digital ecosystems. *Business Horizons, 62*(1), 83-94. doi: https://doi.org/10.1016/j.bushor.2018.08.013

Upadhyay, N. K., & Rathee, M. (2022). Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Medicine, Law & Society, 15*(1), 89-106.

Yuchong, L., & Qinghui, L. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186.