sciendo
Control and Cybernetics
vol. **53** (2024) No. 2
pages: 385-404
DOI: 10.2478/candc-2024-0017

Economic impact of IOT and conventional data breaches: cost analysis and statistical trends*

by

Alisa Harkai and Cristian Eugen Ciurea

Bucharest University of Economic Studies
Piata Romana 6, Bucharest, Romania
cristian.ciurea@ie.ase.ro
harkaialisa22@stud.ase.ro

Abstract: Rapid spread and effective integration of Internet of Things (IoT) devices across various sectors has brought unparalleled connectivity and efficiency, but has also introduced amplified vulnerabilities with respect to data breaches. This article offers an in-depth examination of the economic impacts of IoT data breaches, focusing on the associated costs and emerging statistical trends. Through comprehensive analysis, we explore the direct and indirect financial burdens, including immediate response expenses, long-term reputational damage, legal liabilities, and regulatory penalties. Utilizing recent case studies and statistical data, we highlight the economic magnitude of IoT breaches and the factors that amplify their costs. Our research emphasizes the critical need for enhanced IoT security measures and for strategic risk management to protect organizations from substantial financial losses. The findings may serve as a crucial resource for businesses, policymakers, and cybersecurity professionals, advocating for proactive steps to fortify IoT ecosystems against the escalating threat of data breaches.

Keywords: Internet of Things (IoT), data breaches, IoT vulnerabilities, cost analysis, economic impact

1. Introduction

The Internet of Things (IoT) represents a revolutionary technological advancement (see Lynn et al., 2020), wherein everyday objects are interconnected via

*The lecture, on which the present paper is based, was presented during the BOS/SOR2024 conference in October 2024 in Warsaw, and the paper was accepted for publishing in December 2024.

the internet, enabling them to send and receive data (see Weyrich and Ebert, 2016). This network of interconnected devices, ranging from household items, like smart refrigerators and thermostats to industrial machinery and healthcare monitors, has seen rapid growth and widespread adoption across various sectors. The IoT ecosystem comprises billions of devices globally, creating a vast, dynamic network that enhances efficiency, productivity, and convenience, while producing enormous volumes of data.

The proliferation of the Internet of Things (IoT) brings numerous benefits, such as enhanced connectivity, increased efficiency, and improved convenience across various sectors, including healthcare, manufacturing, and smart homes. However, the widespread adoption of IoT devices often comes with inadequate security measures, making these devices attractive targets for cybercriminals. Unlike traditional IT systems, IoT devices frequently lack robust security protocols, exposing them to significant risks.

Securing a large number of diverse IoT devices is particularly challenging due to the sheer complexity and scale of the IoT networks. These networks can include everything, from simple sensors to complex machinery, each with varying levels of security. This diversity and the interconnectivity of devices increase the overall vulnerability of the IoT ecosystem.

As a result, a noticeable increase in IoT data breaches has been observed. Attackers exploit the existing vulnerabilities to gain unauthorized access to sensitive information, such as personal data and confidential business information, to disrupt critical operations, or even to take control of the devices themselves. These breaches can lead to severe consequences, including financial losses, reputational damage, and operational disruptions.

The growing number of such incidents underscores the urgent need for comprehensive security strategies, that should be specifically tailored to address the unique challenges, which are posed by IoT devices. Effective strategies should include regular security assessments, implementation of advanced security technologies, and development of industry standards, meant to ensure a secure and resilient IoT environment.

It is important to understand the economic impact of data breaches. Direct costs, such as immediate financial loss, and indirect costs, such as damaged reputation and loss of customer trust, can be devastating to affected organizations. Financial resources can be further strained by regulatory fines and compliance costs. Stakeholders can appreciate the value of investing in robust security measures if they understand the economic implications.

This understanding can help inform policy decisions and develop industry standards. Businesses, policymakers and cybersecurity professionals must work together to create a secure IoT environment that encourages innovation and

protects against the potentially serious economic repercussions of a data breach. The purpose of this article is to provide a comprehensive analysis of the economic impact, highlighting cost drivers, statistical trends, and the urgent need to improve Internet of Things security. Although this article emphasizes IoT-related security issues, conventional cases are also analyzed for comparison. Traditional IT systems and their security challenges provide valuable context for understanding the unique vulnerabilities of IoT devices.

2. Background and context

In essence, the Internet of Things (IoT) involves connecting physical objects to a network, allowing them to communicate via the Internet. While the concept of devices interacting with one another has been around for many years, advancements in technology have significantly accelerated its development. Today's sophisticated sensors, accessible data analytics, and cloud computing enable companies to store and process vast amounts of information more efficiently. Additionally, IoT devices have become more affordable and easier to acquire (Nadikattu, 2018). As a result, the widespread adoption of IoT is raising concerns about data privacy and security. Businesses and government entities worldwide are actively working to anticipate and address the potential consequences of using IoT technology with respect to data confidentiality, recognizing the importance of safeguarding the sensitive information (Frustaci, Pace and Aloi, 2017).

The scope of IoT devices is vast and continually expanding, encompassing various sectors and driving innovation in automation, production and organization efficiency, and data-driven decision-making. From enhancing everyday consumer experiences to revolutionizing industrial operations and healthcare services, the IoT's impact is far-reaching and transformative. The applications for IoT devices (Vongsingthong and Smanchat, 2014) are typically categorized into consumer, commercial, industrial, and infrastructure domains. Within the consumer space, IoT devices are integral to home automation, encompassing systems for lighting, heating and air conditioning, media, and security (Perera, Liu and Jayawardena, 2015). Smart homes (Kang, Moon and Park, 2017) or automated homes can be managed through platforms or hubs that control various smart devices and appliances.

In the financial sector, IoT is revolutionizing the manner, in which the services are delivered and managed. IoT devices enable real-time tracking of financial transactions, enhance the security of online banking through biometric authentication, and provide personalized customer experiences via smart ATMs and wearable payment devices. Additionally, financial institutions use IoT data analytics to gain insights into consumer behavior, optimize operations, detect

fraud, and improve risk management. Then, in the medical field, the Internet of Medical Things (IoMT) represents a significant domain of application of IoT technology, focusing on health-related purposes, data collection, research, and patient monitoring. Often referred to as "Smart Healthcare" (Kricka, 2019; Gatouillat et al., 2018) IoMT aims to create a digitized healthcare system by connecting medical resources and healthcare services efficiently. Further, transportation systems also benefit from IoT applications, extending to vehicles, infrastructure, and users. Examples include smart traffic control, smart parking, electronic toll collection, logistics and fleet management, vehicle control, safety enhancements, and road assistance. Additionally, IoT devices are used to monitor and control mechanical, electrical, and electronic systems in various types of buildings, including public, private, industrial, institutional, and residential structures, through home and building automation systems.

As these devices become more integral to daily operations and personal lives, it is crucial to understand the associated security risks. Given the vast and diverse nature of IoT networks, ensuring robust security measures is paramount. However, the very features that make IoT devices so beneficial—such as their connectivity and accessibility—also introduce significant vulnerabilities. This leads us to explore the IoT data breaches and the common vulnerabilities that these devices face.

A data breach is a security incident that happens when unauthorized individuals or organizations gain access to private, confidential, or proprietary information. They could pull out things such as Social Security numbers, credit card details and health information, along with company stuff, such as ideas about details (often not shared) about customers and financial reports. Various things can cause these breaches to happen, such as online attacks, hidden insider threats, or just mistakes that leak the respective information. When this happens, a breach can damage a person's bank account, lead to legal issues, or harm personal reputation or that of businesses (IBM, 2024).

It is important to know that not every type of cyberattack is a data breach. Data breaches specifically refer to attacks, where unauthorized individuals or entities gain access to data. For example, a DDoS attack is not a data breach. However, a ransomware attack is definitely a type of data breach, because it locks data and extorts the affected companies and individuals by threatening to steal their data if a ransom is not paid. Additionally, if someone steals a USB drive or another physical storage medium, it can also be considered a data breach.

Now that we have defined and understood what a data breach is, let us move on to defining and detailing what causes these types of attacks. There are three main categories of reasons why data breaches occur: accidental mistakes,

malicious insiders, and hackers. Each of these categories encompasses a range of specific scenarios that contribute to the occurrence of data breaches.

Accidental mistakes often happen due to human error or lack of awareness. These can include:

- **Misdirected emails:** Sending sensitive information to the wrong recipient by mistake.
- **Weak passwords:** Using simple, easily guessable passwords that can be easily cracked.
- **Unsecured networks:** Accessing sensitive data over unsecured Wi-Fi networks, exposing it to interception.
- **Improper disposal of data:** Failing to properly destroy old documents or electronic devices containing sensitive information.

Malicious insiders are individuals within an organization who exploit their access to sensitive data for personal gain or to harm the organization. These can include:

- **Disgruntled employees:** Current or former employees who steal data to retaliate against the company.
- **Corporate espionage:** Employees who sell confidential information to competitors.
- **Privileged access abuse:** Individuals with high-level access who misuse their privileges to extract sensitive data.

Hackers are external individuals or groups who use various techniques to gain unauthorized access to systems and data. These can include:

- **Phishing attacks:** Sending fraudulent emails to trick individuals into providing sensitive information or downloading malware.
- **Malware and ransomware:** Installing malicious software that can steal data or lock systems until a ransom is paid.
- **Exploiting vulnerabilities:** Finding and exploiting security weaknesses in software or hardware to gain access to data.
- **Brute force attacks:** Using automated tools to guess passwords and break into accounts.

3. Economic impact analysis

3.1. The overall image

Moving forward, we will now explore the top 15 data breaches in 21^{st} century, examining their impact by describing in more detail the chart, which is shown in Fig. 1.

Following an article, written in 2022 and published on CSO (CSO, 2022), our research has identified the most impactful data breaches of the 21st century to date. The data presented originate from 2021, as it is the year, in which companies responded to the statistical study referred to. Through the research here quoted, we can identify the significant data breaches that have occurred over the past decade.

In the chart in Fig. 1, we have included all 15 data breaches in chronological order, starting from the year 2012 up till 2021. Each entry details the name of the company involved in the breach for the respective year. Additionally, we have provided an assessment of the impact of each data breach, which is expressed in terms of millions of users or accounts affected.

This impact measurement helps to quantify the extent of each breach, highlighting the substantial number of individuals impacted.

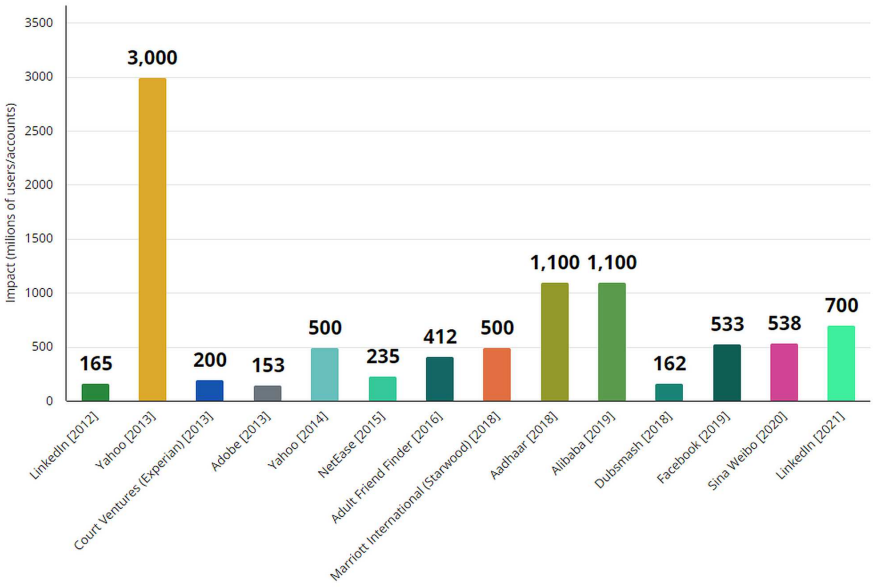

Figure 1. Top 15 data breaches of the 21st century. Source: own elaboration of the authors on the basis of CSO (2022)

Further, through our study, we aim to highlight two more top lists of the largest data breaches, this time from the years 2023 and 2024. We will present the data in Tables 1 and 2, respectively.

Table 1 presents the largest data breaches of 2024 on a global scale. It includes comprehensive information such as the country, where the affected

company is located, the sector impacted by the breach, the total number of records stolen, and the specific month in 2024 when each incident occurred. This detailed overview allows for a better understanding of the geographic and sectoral trends in data breaches.

Then, in Table 2, we provide analogous data concerning the largest data breaches from both 2023 and 2024 within Europe, explicitly excluding Russia. This table will highlight similar metrics, providing insights into the trends and patterns of data breaches in the European context, further enriching our analysis by allowing for the comparisons with the previously mentioned global incidents, listed in Table 1. We would like to emphasize that all data presented in both Table 1 (IT Governance, 2024a) and Table 2 (IT Governance, 2024b) has been sourced from the IT Governance website. This information reflects accurate findings derived from their research studies and statistical reports.

We must understand that securing our networks and information systems, especially as companies, is of paramount importance. The lack of adequate security measures can lead to significant damage, as demonstrated by the concrete cases highlighted in the two tables above. These tables illustrate the catastrophic outcomes of data breaches, showcasing millions of affected records. Unfortunately, these figures also translate into substantial costs, which inevitably accompany the resulting issues.

From an economic impact perspective, the costs associated with these data breaches can be divided into three major categories: direct costs, indirect costs, and regulatory costs. Direct costs encompass immediate expenses such as forensic investigations, notification of affected parties, legal fees, and remediation efforts. Indirect costs refer to long-term repercussions, including loss of customer trust, business disruption, reputational damage, and potential increases in insurance premiums. Regulatory costs involve fines and penalties imposed by authorities, compliance audits, and the expenses associated with meeting regulatory requirements.

To provide a clearer understanding, we will detail each of the three types of costs associated with data breaches as follows:

3.2. Direct costs

Direct costs are the immediate and tangible expenses incurred as a result of a data breach. These costs include:

- **Forensic investigations:** Engaging cybersecurity experts to determine the cause, scope, and impact of the breach. This often involves extensive data analysis and system audits to uncover vulnerabilities.
- **Notification costs:** Informing affected individuals and stakeholders about

Table 1. Top 10 global data breaches of 2024. Source: own elaboration of the authors on the basis of IT Governance (2024a)

No.	Company	Sector	Location	Records breached	Month (2024)
1	MOAB	Multiple	Multiple	>26,000,000,000	January
2	Discord (via Spy.pet)	IT	USA	4,186,879,104	April
3	Far Eastern Research Center for Space Hydrometeorology	Public	Russia	2 PB (Peta Bytes)	January
4	Honor, Xiaomi, OPPO, Huawei, Baidu	IT	China	Up to 1,000,000,000	April
5	Indian mobile network consumer database	Telecom	India	750,000,000	January
6	Zenlayer	Telecom	USA	384,658,212	February
7	Unknown Brazilian organisation	Unknown	Brazil	>223,000,000	January
8	Telekom Malaysia	Telecom	Malaysia	Almost 200,000,000	January
9	Pure Incubation Ventures	Professional services	USA	183,754,481	February
10	916 Google Firebase websites	Multiple	USA	124,605,664	March

Table 2. Top 6 data breaches of 2023-2024 in Europe. Source: own elaboration of the authors on the basis of IT Governance (2024b)

No.	Company	Sector	Location	Records breached	Month
1	SAP SE Bulgaria	IT	Bulgaria	92,592,696	November 2023
2	France Travail	Public	France	43,000,000	March 2024
3	MX3 Nutrition	Manufacturing	France	36,000,000	March 2024
4	Viamedis and Almerys	Healthcare	France	>33,000,000	February 2024
5	Tecnoquadri Srl	Manufacturing	Italy	33,000,000	December 2023
6	EasyPark	IT	UK	21,100,000	December 2023

the breach, which may involve mailing notifications, setting up call centers, and providing credit monitoring services to those impacted.

- **Remediation expenses:** Costs to restore and secure systems, including patching vulnerabilities, updating software, and enhancing security protocols to prevent future breaches.
- **Public relations and customer support:** Allocating resources to manage public relations campaigns, addressing customer concerns, and mitigating reputational damage through crisis management strategies.

These direct costs are often substantial and the corresponding issues must be addressed promptly to contain the damage and prevent further losses.

3.3. Indirect costs

Indirect costs are less immediate but have a significant long-term impact on the organization's operations and reputation. They include:

- **Business interruption:** Downtime and operational disruption that occur while systems are being restored and secured. This can lead to lost revenue, decreased productivity, and delayed business activities.
- **Reputational damage:** Loss of customer trust and brand credibility, which can result in decreased sales, loss of market share, and long-term

damage to the company's reputation. Rebuilding trust with customers and stakeholders can be a prolonged and costly process.
- **Increased insurance premiums:** Following a breach, organizations may face higher insurance premiums for cybersecurity coverage due to the perceived increased risk. This can significantly raise the cost of maintaining adequate insurance protection.
- **Employee morale and turnover:** The breach can create internal turmoil, leading to decreased employee morale, increased stress, and potential turnover. The costs associated with recruiting and training new staff can be considerable.

These indirect costs can erode an organization's financial stability and weaken its competitive position over time.

3.4. Regulatory costs

Regulatory costs arise from non-compliance with data protection laws and regulations. They include:

- **Fines and penalties:** Financial penalties imposed by regulatory bodies for failing to protect personal data or for violating data breach notification laws. These fines can be substantial, depending on the jurisdiction and the severity of the breach.
- **Compliance audits and legal compliance:** Costs associated with conducting internal audits, assessments, and obtaining certifications to ensure ongoing compliance with data protection regulations. This may also involve hiring external consultants and legal experts to review and enhance compliance measures.
- **Lawsuit settlements and legal costs:** Expenses related to settlements with affected parties or regulatory bodies, including court fees, litigation costs, and settlements. These costs can be significant, especially in cases involving large-scale data breaches.
- **Reputational scrutiny:** Increased scrutiny from regulatory authorities and the potential for heightened regulatory oversight in the aftermath of a breach. This can lead to ongoing compliance obligations and increased regulatory costs.

Understanding these categories helps highlight the comprehensive economic impact of data breaches, underscoring the necessity for robust security measures to protect sensitive information and mitigate potential financial losses.

This empirically motivated research has helped us better understand the categories of costs that apply and how they directly and/or indirectly influence the consequences of these data breaches. For a company, especially one at a multinational level, it is crucial to avoid these data breaches as much as

possible or, if they cannot be completely avoided, to minimize them to a very large extent, because otherwise, they risk losing an enormous amount of money. Moving forward, we will practically examine what it means to face data breaches and the costs that arise as a result.

3.5. Trends in costs of breaches

In the present subsection, we will focus strictly on the practical side, specifically the costs associated with data breaches. Firstly, we must mention that all data that we do present here has been collected from a report conducted by IBM in 2023 (IBM, 2023), which includes historical data up to and including the year 2023. Data for 2024 and future forecasts will be presented after the data from previous years. Additionally, we should note that while the data was collected from IBM, all graphical illustrations have been created by the authors.

We begin by presenting the overall cost of data breaches globally, as illustrated in Fig. 2.

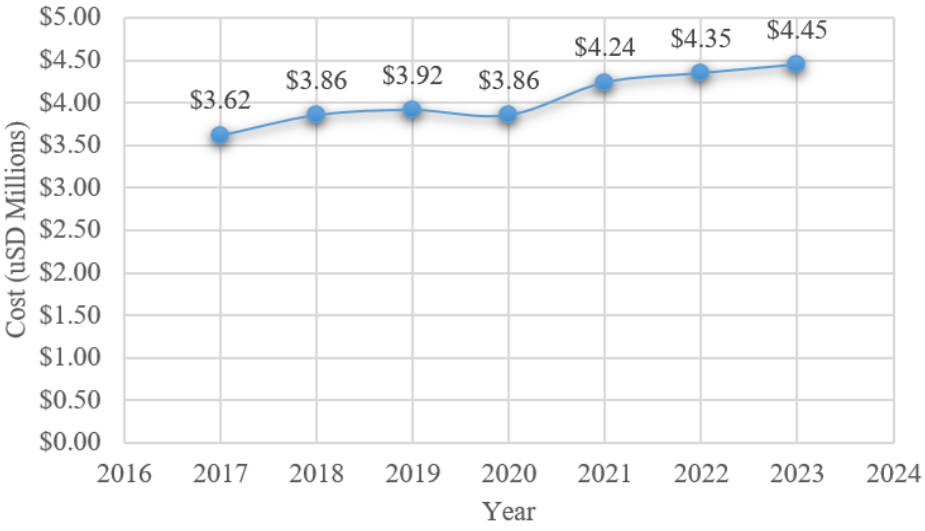

Figure 2. Average total cost of data breaches globally (2017-2023). Source: own elaboration of the authors on the basis of IBM (2023)

We can see that starting from the first year analyzed, 2017, the costs associated with global data breaches have increased each year, with the exception of 2020, when there was a decrease compared to 2019, which can be definitely associated with the impact of the COVID-19 pandemic (note, though, that nominal

values are considered here, not adjusted for inflation). However, costs began to rise again in 2021. On a global scale, the average cost of a data breach climbed to USD 4.45 million, marking an increase of USD 100,000 from 2022. This change signifies a 2.3% rise compared to the 2022 average cost of USD 4.35 million. From 2020, when the average total cost of a data breach was USD 3.86 million, the average cost has surged by 15.3%.

Next, we continue discussing costs by showing in Fig. 3 a cost analysis juxtaposing the differences between the years 2022 and 2023 for selected regions of the world.

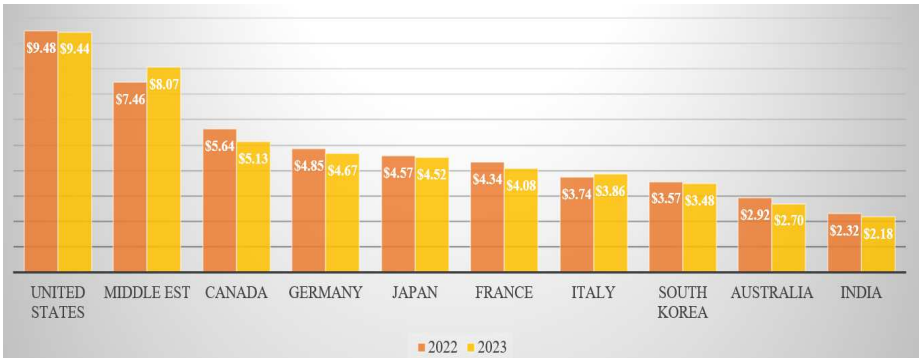

Figure 3. Analysis of data breach cost between 2022 and 2023 by region. Source: own elaboration of the authors on the basis of IBM (2023)

The analyzed report, IBM (2023), whose results are shown in Fig. 3, provides the information on the cost of data breaches in 2022 across the regions or countries mentioned in the figure, compared to the costs caused by the same source of cybersecurity incidents in 2023 for the same regions or countries. We can clearly observe that the 2023 statistics are almost universally more favorable than those from 2022, as the costs have generally decreased, with the exception of the Middle East. However, the perspective on this decrease matters. If we consider that costs have gone down because companies and individuals in those countries implemented better security measures against data breaches, resulting in fewer incidents and therefore fewer associated repair costs, this is a positive development. Conversely, if the costs have decreased merely because these entities have paid less attention to the aftermath of data breaches and have not responded as rigorously, then the lower costs may not be as positive.

To avoid being pessimistic and to assume that companies have indeed taken appropriate actions, we will consider the first scenario more deeply. We now move on to Fig. 4, which similarly highlights costs associated with data breaches, but this time categorized by the affected industries.

According to the data that are represented in Fig. 4, healthcare continues for 13^{th} year in a row (since 2011) to endure the highest data average breach costs among all industries, rising from USD 10.10 million in 2022 to USD 10.93 million in 2023, which corresponds to 8.2% of increase. Over the last three years, the average cost of a data breach in healthcare has surged by 53.3%, climbing by more than USD 3 million compared to the 2020 average of USD 7.13 million. The healthcare sector faces stringent industry regulations and is deemed critical infrastructure by the US government. Since the onset of the COVID-19 pandemic, this industry has experienced significantly higher average data breach costs.

The top five of the most costly industries, in this context, have seen some changes from the previous year's rankings. The technology sector dropped out of the top five, while the industrial sector was added, showing a 5.8% increase as it moved from the seventh rank to the fifth. According to IBM threat intelligence, manufacturing has become the industry that was most frequently targeted by the cybercriminals.

In 2023, cyberattacks, such as, in particular, data breaches and account takeovers, caused the estimated global loss of 8 trillion USD. This amount is forecasted to rise to 9.5 trillion USD for the year 2024, according to Cybersecurity Ventures. The growth of AI technology is anticipated to further escalate these costs, with projections indicating an 11% increase, bringing the total to 10.5 trillion USD by 2025 (see ExpressVPN, 2024).

Next, we will delve into the forecasted figures, related to the economic impact of data breaches. Drawing from a comprehensive study, conducted by Statista and Cybersecurity Ventures (see ExpressVPN, 2024), Table 3 provides detailed projections of data breach costs within the period from 2024 to 2030. These projections offer valuable insights into the anticipated financial trends and potential economic burden that organizations worldwide may face in the context of the escalating cyber threats.

The projections, summarized in Table 3, consider technological progress, industry patterns, and potential global events that could influence the cost of cybercrime. As both cybercriminals and cybersecurity professionals continuously innovate their tools and methods, the expenses and effectiveness of both attacks and defense strategies are affected. Additionally, geopolitical circumstances and economic conditions can alter the frequency and characteristics of cyberattacks, significantly adding to the complexity of the cost forecasts (ExpressVPN, 2024).

According to these studies and the related future projections, the issue extends beyond the increasing number of cyberattacks. Unfortunately, consumers will bear the costs in two significant ways. Firstly, their personal data will be at greater risk of being compromised, and their devices may be subject to various forms of cyberattacks. Secondly, they will face higher financial costs. As

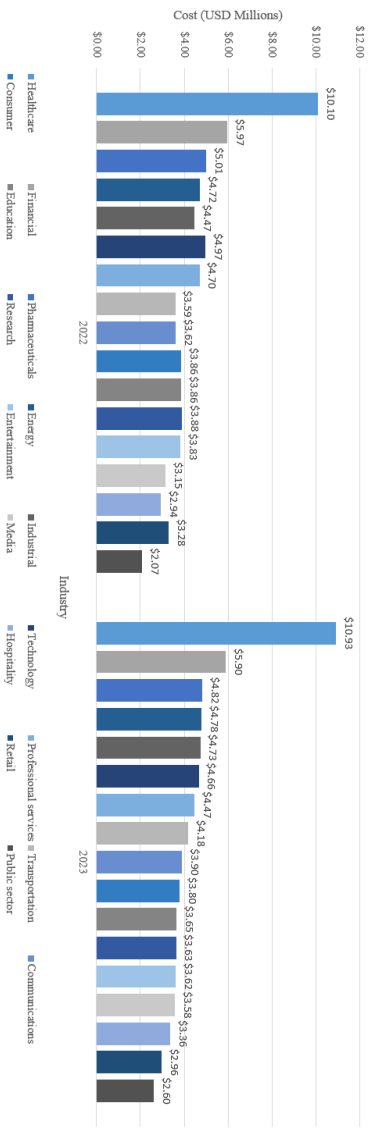

Figure 4. Analysis of average data breach costs between 2022 and 2023, by industry. Source: own elaboration of the authors

Table 3. Estimated annual cost of cyberattacks globally (2024-2030)

Year	Estimated annual cost of cyber attacks globally (measured in trillions of USD)	Increase from the previous year (%)
2024	$9.5 trillions	19%
2025	$10.5 trillions	10.5%
2026	$11.3 trillions	7.6%
2027	$12.4 trillions	9.7%
2028	$13.8 trillions	11%
2029	$15.6 trillions	13%
2030	$17.9 trillions	15%

Source: own elaboration of the authors

cyberattacks become more prevalent, the prices of IT products and services are expected to rise. This increase will likely affect subscription fees for various services and licenses for IT products, ultimately leading to higher expenses for consumers.

4. Mitigation strategies and best practices

In order to effectively prevent the data breaches and to mitigate their economic impact, organizations must, definitely, adopt a comprehensive and multi-layered approach. This involves implementing a range of preventive measures, maintaining vigilant monitoring, and having a well-prepared response strategy.

Robust cybersecurity measures

Organizations should deploy advanced firewalls and antivirus software to create a strong defense against unauthorized access and malware. Firewalls act as a barrier between internal networks and external threats, while antivirus software detects and removes malicious software before it can cause harm. Additionally, data encryption should be applied both in transit and at rest. Encryption ensures that sensitive information remains unreadable without the proper decryption key, even if intercepted by attackers. Secure configuration of systems is also crucial; this means disabling unnecessary features and services that might be exploited by attackers. Regular updates and patches should be applied to all software and systems to protect against known vulnerabilities.

Strengthening access controls

Implementing multi-factor authentication (MFA) provides an additional layer of security, extending beyond just the passwords. MFA requires users to provide multiple forms of verification, such as a password and a biometric scan, making unauthorized access significantly more difficult. Adoption of the principle of least privilege ensures that users are granted only the permissions necessary to perform their job functions, thereby minimizing the potential access points for attackers. Regular access reviews should be conducted to adjust permissions as needed, ensuring that former employees and other unauthorized individuals do not retain access to sensitive systems.

Regular security audits and assessments

Conducting regular vulnerability assessments and penetration tests helps to identify potential weaknesses before they can be exploited. These assessments simulate attacks to uncover vulnerabilities in systems and applications. Comprehensive security audits should also be carried out to evaluate the effectiveness of existing security policies and practices. A robust patch management process is essential for applying security patches and updates to software and systems promptly, thereby addressing known vulnerabilities and reducing the risk of exploitation. Responsibility for conducting regular vulnerability assessments and penetration tests depends on the service model and agreements in place. Typically, customers are responsible for their internal systems, while providers handle the security of hosted or managed environments.

Employee education and training

Security awareness training is vital for educating employees about common threats, like phishing attacks and social engineering tactics. Training should include recognizing suspicious emails, avoiding clicking on unknown links, and reporting potential threats. Incident response drills are essential for preparing employees to handle security incidents effectively. These drills simulate real-world scenarios and help employees practice their response to data breaches or other security events. Phishing simulations are useful for testing and improving employees' ability to recognize and respond to phishing attempts.

Incident response planning

Developing a detailed incident response plan is crucial for managing data breaches effectively. This plan should outline the steps to be taken during a breach, including roles and responsibilities, communication strategies, and containment

measures. Establishing a dedicated incident response team ensures that there is a clear structure for managing and resolving security incidents. A communication strategy must be in place so as to manage both internal and external communications, including notifying affected parties and regulatory bodies in accordance with legal requirements.

Data governance and management

Data classification involves categorizing data based on its sensitivity and importance, which helps in applying appropriate protection measures. Implementing data minimization practices ensures that only the necessary amount of personal data is collected and retained for business purposes, reducing the risk, associated with data breaches. Secure data disposal methods should be used to ensure that sensitive data is properly destroyed or deleted, preventing unauthorized access to information that is no longer needed.

Continuous monitoring and threat detection

Security Information and Event Management (SIEM) systems are instrumental in monitoring and analyzing security events in real-time. These systems provide a centralized view of security data, enabling faster detection and response to potential threats. Staying informed about emerging threats through threat intelligence feeds and industry reports helps organizations anticipate and prepare for new risks. Implementation of anomaly detection tools helps in identifying unusual patterns of activity that may indicate a security incident, allowing for prompt investigation and response.

Compliance with regulations

Adhering to data protection regulations such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), and HIPAA (Health Insurance Portability and Accountability Act) is essential for legal compliance and mitigation of the risk of fines and penalties. Regular reviews should be conducted to ensure ongoing compliance with relevant laws and standards. These regulations often dictate specific requirements for data protection and breach notification, and maintaining compliance helps protect organizations from legal and financial repercussions.

Investing in cybersecurity insurance

Cybersecurity insurance can provide financial protection against losses resulting from data breaches and other cyber incidents. Organizations should carefully evaluate their insurance needs and consider policies that cover a wide range of potential threats. Regularly reviewing and updating the insurance policy ensures that it remains adequate as the organization's risk profile evolves.

By adopting these comprehensive strategies, organizations can significantly reduce their vulnerability to data breaches and minimize the associated economic damage. It is, of course, necessary to carry out an in-depth analysis of the risks and costs associated, in order to design and then undertake a policy and strategy that truly minimize the expected costs, even though at a glance we might have the impression that we deal with actual and precise costs (of the security measures) versus the uncertain, expected costs of breaches and other intrusions. Yet, in fact, there is only a difference of certainty between these two categories at the instant of undertaking planning and design.

5. Future outlook

As we look to the future, several important trends are shaping as to how we prevent and manage data breaches. Advances in cybersecurity technology are at the forefront of this evolution. With the integration of artificial intelligence and machine learning, organizations will have better tools to detect and respond to threats in real time. These technologies are capable of analyzing vast amounts of data to identify unusual patterns and adapt to new types of attacks, thereby enhancing overall security.

Another significant shift is the growing adoption of Zero Trust architecture. This model emphasizes continuous verification of all users and devices, rather than relying solely on perimeter defenses. By enforcing strict access controls and validating every request, Zero Trust helps to minimize vulnerabilities and reduce the risk of unauthorized access.

As data privacy regulations become more stringent around the world, organizations will need to keep up with evolving laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Ensuring compliance will involve regularly updating security practices to meet these legal requirements.

Quantum computing represents both an opportunity and a challenge. While it promises to revolutionize data processing, it also threatens current encryption methods. Preparing for this future will involve developing new encryption technologies that can withstand quantum attacks.

6. Conclusions

The integration of Internet of Things (IoT) devices will continue to expand, making it crucial to secure these endpoints. Future strategies will focus on robust authentication processes, secure device management, and timely updates to address potential vulnerabilities. The cyber insurance market is also expected to grow, as organizations seek financial protection against data breaches. Insurers will likely demand detailed security practices from clients and offer policies that cover emerging threats. Supply chain security will be increasingly important as well. Organizations will need to enhance their measures for vetting and monitoring third-party vendors to ensure comprehensive protection across their supply chains.

Finally, cultivating a strong security culture within organizations will be essential. Ongoing training and a shared sense of responsibility for security will help minimize risks and improve adherence to best practices.

In conclusion, while the landscape of data breaches will continue to change, staying ahead of these trends and adopting proactive measures will be key to effectively managing and mitigating future risks.

References

ExpressVPN (2024) The true cost of cyber attacks in 2024 and beyond https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/. (accessed 15th July 2024).

Frustaci, M., Pace, P. and Aloi, G. (2017) Securing the IoT World: Issues and Perspectives. In: *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 246–251.

Gatouillat, A., Badr, Y., Massot, B. and Sejdic, E. (2018) Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine. *Journal of Healthcare Engineering*. IEEE, **5**, 3810–3822.

IBM (2023) *Cost of a Data Breach Report 2023*. https://www.ibm.com/security/data-breach (accessed 30th June 2024)

IBM (2024) What is a data breach? https://www.ibm.com/topics/data-breach (accessed 30th June 2024).

IT Governance (2024a) Global Data Breaches and Cyber Attacks in 2024, https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024 (accessed 12th July 2024).

IT Governance (2024b) Data Breaches and Cyber Attacks – Europe 2024 Report, https://www.itgovernance.eu/blog/en/data-breaches-and-cyber-attacks-in-2024-in-europe (accessed 12th July 2024).

Kang, W. M., Moon, S. Y. and Park, J. H. (2017) An Enhanced Security

Framework for Home Appliances in Smart Homes. *Human-Centric Computing and Information Sciences*, **7** (6), https://doi.org/10.1186/s13673-017-0087-4

Kricka, L. J. (2019) History of Disruptions in Laboratory Medicine: What Have We Learned from Predictions? *Clinical Chemistry and Laboratory Medicine*. **57**(3), 308–311.

Lynn, T., Endo, P.T., Ribeiro, A.M.N.C., Barbosa, G.B.N., and Rosati, P. (2020) The Internet of Things: Definitions, Key Concepts, and Reference Architectures. In: T. Lynn, J. Mooney, B. Lee and P. Endo, eds., *The Cloud-to-Thing Continuum*. Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-41110-7_1. https://link.springer.com/chapter/10.1007/978-3-030-41110-7_1#citeas

Nadikattu, A. K. R. (2018) IoT and the Issue of Data Privacy. *Journal of Advances in Computer Engineering and Technology*, **5**(10). ISSN: 2394–3696.

Perera, C., Liu, C. H. and Jayawardena, S. (2015) The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey. *IEEE Transactions on Emerging Topics in Computing*, **3**(4), 585–598. DOI: 10.1109/TETC.2015.2390034

Vongsingthong, S. and Smanchat, S. (2014) Internet of Things: A Review of Applications & Technologies. *Suranaree Journal of Science and Technology*, **21**(4):359-374.

Weyrich, M. and Ebert, C. (2016) Reference Architectures for the Internet of Things. *IEEE Software*, **33**(1), 112–116. https://doi.org/10.1109/MS.2016.20