Cybersecurity-level assessment models

Tetiana Babenko[1,2,†], Saule Amanzholova[3,†], Rostyslav Lisnevskyi[1,†] and Aisha Abylgazy[1,†]

[1] International Information Technology University, 34/1 Manas St., Almaty, 050000, Kazakhstan
[2] Taras Shevchenko National University of Kyiv, 64/13 Volodymyrska Street, Kyiv, 01601, Ukraine
[3] Astana IT University, Astana, Kazakhstan

Abstract

This study presents the development of an adaptive model for evaluating the level of cybersecurity in an organization. The model is aimed at improving the efficiency and accuracy of control assessments within the information security management system (ISMS), with a focus on automating and simplifying the metrics outlined in the ISO/IEC 27004:2016 standard. By applying both qualitative and quantitative methods, the model enables a comprehensive analysis of the current state of cybersecurity and the effectiveness of control implementation. One of the key findings of the study is the ability to automate approximately 30% of the controls, which significantly enhances operational efficiency, reduces manual tasks, and improves data collection quality. The practical significance of the research lies in the fact that implementing this model will not only improve the organization's cybersecurity level but also ensure continuous improvement of information security processes.

Keywords

cybersecurity, Adaptive Measurement Model, ISO/IEC 27004:2016, Information Security Management System (ISMS), Control Automation, Cybersecurity Evaluation, Continuous Improvement, Qualitative and Quantitative Methods

1. Introduction

The field of cybersecurity has evolved significantly over the past few decades, becoming a critical aspect of organizational risk management. As cyber threats continue to grow in both frequency and sophistication, companies must constantly adapt and invest in robust cybersecurity measures. The dynamic nature of cyberspace—where new vulnerabilities are continuously discovered, and threat actors develop ever-more advanced methods of exploitation—necessitates the implementation of proactive security strategies. Failure to do so can result in catastrophic breaches, loss of sensitive data, financial damage, and long-term reputational harm.

In light of these growing threats, organizations are increasingly adopting data-driven strategies to gain valuable insights into their cybersecurity posture. This approach allows companies to systematically assess the effectiveness of their security controls, identify gaps, and make informed decisions regarding resource allocation. In fact, recent statistics show that seven out of the ten most valuable enterprises rely heavily on data to guide key decisions across various business functions, including cybersecurity [1]. Data-driven decision-making, especially in cybersecurity, enables organizations to react more swiftly to emerging threats, improve their incident response times, and ensure that their protective measures remain effective over time.

However, implementing a data-driven strategy specifically for cybersecurity poses unique challenges. Unlike more straightforward business processes, cybersecurity involves a highly complex set of dynamic variables, including threat intelligence, vulnerabilities, user behavior, and external regulatory requirements. The development of meaningful, quantifiable metrics for cybersecurity

DTESI 2024: 9th International Conference on Digital Technologies in Education, Science and Industry, October 16–17, 2024, Almaty, Kazakhstan
* Corresponding author.
† These authors contributed equally.
t.babenko@iitu.edu.kz (T. Babenko); s.amanzholova@astanait.edu.kz (S. Amanzholova) r.lisnevskyi@iitu.edu.kz (R. Lisnevskyi); a.abylgazy@iitu.edu.kz (A. Abylgazy)
0000-0003-1184-9483 (T. Babenko); 0000-0002-6779-9393 (S. Amanzholova); 0000-0002-6779-9393 (R. Lisnevskyi); 0000-0002-9006-6366 (A. Abylgazy)

remains a significant hurdle. While well-established Key Performance Indicators (KPIs) exist for day-to-day security operations, defining metrics for high-level cybersecurity management processes is more difficult.

Cybersecurity KPIs must go beyond simply tracking the number of incidents or average response times. To provide a comprehensive assessment, these metrics need to address the overall efficiency, effectiveness, and robustness of an organization's Information Security Management System (ISMS). An effective ISMS not only protects the organization's information assets but also ensures compliance with various standards and regulations, such as ISO/IEC 27001.

Guidelines for implementing and measuring ISMS performance are outlined in the ISO/IEC 27004 standard [2]. This standard provides organizations with a set of metrics and indicators to monitor, measure, and evaluate their ISMS. These metrics help organizations assess whether they are meeting their cybersecurity objectives, enabling them to take corrective actions when necessary.

Moreover, regular measurement of ISMS performance aids in continuous improvement, ensuring that the system evolves in response to new threats.

While ISO/IEC 27004 offers a comprehensive framework, many organizations face significant challenges in fully implementing it. Some of the key challenges include:

- Complexity: The standard is extensive and includes numerous prerequisites that can be difficult to fully comprehend and satisfy.
- Resource Constraints: Implementing ISO/IEC 27004 requires substantial resources, including skilled personnel, time, and financial investment. Many organizations, particularly small and medium-sized enterprises (SMEs), struggle with allocating the necessary resources.
- Lack of Expertise: Implementing an ISMS and accurately measuring its performance often requires specialized expertise that many organizations lack. The absence of knowledge in both security management and metric development hinders the proper application of ISO/IEC 27004.
- Resistance to Change: Many organizations face resistance when attempting to modify existing processes to align with ISO/IEC 27004, particularly when these changes impact workflows or require additional investments.
- Senior Management Support: The success of ISMS implementation hinges on support from senior management. Without their commitment, prioritizing security efforts and securing the necessary resources becomes difficult.

Despite these challenges, the implementation of ISO/IEC 27004 remains a crucial step for organizations striving to maintain a high level of cybersecurity. The adoption of standardized metrics and indicators not only enhances operational efficiency but also provides a common language for evaluating cybersecurity performance. By leveraging these metrics, organizations can gain a clearer understanding of their security posture and continuously improve their defenses against evolving threats.

2. Literature overview

Managing information security in modern organizations has become a complex and resource-intensive challenge. This complexity stems from the continuous evolution of cyber threats, regulatory requirements, and the increasing integration of digital technologies into business processes. As organizations strive to protect their information assets, various models and frameworks have been developed to support the implementation, measurement, and evaluation of cybersecurity controls. Among these, the ISO/IEC 27001 and ISO/IEC 27004 standards stand out as foundational guidelines for building and assessing effective Information Security Management Systems (ISMS).

A previous study [4] analyzed the feasibility of automating certain security controls within the context of ISO/IEC 27001. The research found that not all controls can be fully automated due to the

inherent complexity of some security processes. The criteria for determining whether a control can be automated are based on the following factors:

The control can be partially or fully implemented using one or more security systems, such as Security Information and Event Management (SIEM) systems, Endpoint Protection, or Network Access Control systems.

The control can be operated and monitored by machine-readable and processable resources, whereas human-oriented controls (e.g., security awareness training) cannot be automated, as they require human interaction and decision-making.

The study concluded that approximately 30% of the controls outlined in ISO/IEC 27001 could be automated, with the remainder requiring human oversight. This finding underscores the complexity of balancing automation with human involvement in cybersecurity management. Moreover, the integration of multiple cybersecurity systems is necessary to automate these controls effectively, adding another layer of complexity to the process. Automation also brings its own set of challenges related to the ongoing measurement and monitoring of these controls, which must be regularly evaluated to ensure they remain effective.

In another study, an Information Security Measurement Infrastructure for KPI Visualization was developed [5]. This study presented a technical architecture that supports the collection, mining, and presentation of key performance indicators (KPIs) related to information security. The infrastructure leveraged open-source visualization tools to provide a comprehensive view of an organization's security posture. However, one of the primary challenges identified was the need for significant manual customization to ensure the relevance and accuracy of the collected data. This highlights a broader issue: even when automated systems are implemented, manual intervention and expertise are often required to fine-tune the results and ensure the validity of the measurement process.

An alternative approach to measuring the effectiveness of information security management controls was introduced in [6]. This study focused on developing a step-by-step process for determining the measurement object, the parameters to be measured, and the corresponding metrics. The research aimed to simplify the process of identifying key attributes and metrics, thus reducing the complexity of security assessments. However, the study noted that while the creation of measurement techniques is important, there is still a need for a holistic evaluation process that encompasses the full spectrum of cybersecurity risks and controls.

Other studies have focused on the performance assessment of ISMS implementations. For instance, research [7] introduced a process-oriented assessment system for measuring the efficiency of ISMS operations. The system provided upper and lower bounds for calculating efficiency based on existing risks and statements of applicability. By mapping these risks to specific controls, organizations can better understand their security posture and identify areas where improvements are necessary. The study also employed a Total-Cost-of-Ownership (TCO) model, which accounted for both direct and indirect costs, as well as operational expenses, when evaluating the efficiency of security measures. This comprehensive approach allowed for a more detailed analysis of the economic impact of implementing and maintaining security controls.

In the context of cybersecurity optimization, a survey of various models for evaluating cyberinfrastructure security was presented in [8]. This study reviewed different approaches to assessing the security of critical infrastructures, focusing on performance matrices that help organizations prioritize and optimize their security measures. By combining these models with the ISO/IEC 27004 framework, organizations can gain a more complete understanding of their security vulnerabilities and develop strategies to address them.

Research on the organizational variables influencing the successful implementation of ISO/IEC 27001 was presented in [9]. This study identified four key variables—IT managerial skill, environmental uncertainty, industry type, and organizational size—that significantly impact the implementation and effectiveness of information security management. The findings suggest that larger organizations with well-developed IT departments are more likely to successfully implement ISO/IEC 27001 compared to smaller organizations, which often lack the necessary resources and

expertise. Additionally, industries facing higher levels of environmental uncertainty, such as finance or healthcare, tend to invest more heavily in information security controls.

The Security Requirements Engineering Process Framework was introduced in [10], offering a structured approach to defining and prioritizing security requirements. This framework includes activities such as:

1. Setting the security vision,
2. Identifying the stakeholders and their security needs,
3. Recognizing the organization's assets and vulnerabilities,
4. Establishing security objectives and corresponding threats,
5. Conducting risk assessments and prioritizing security requirements based on potential impact.

This framework provides a clear methodology for establishing a security vision and ensuring that the identified requirements are aligned with the organization's broader security goals.

Another study [11] proposed a model for developing security assurance and risk management processes within an ISMS, incorporating intrusion prevention capabilities. This framework enhanced the organization's ability to manage risks by providing mechanisms for preventing, detecting, and responding to security incidents in real time. The integration of intrusion prevention with broader ISMS functions represents an important development in the field of risk management, as it ensures that organizations can respond quickly to emerging threats while maintaining compliance with established standards.

In the realm of audit planning, research [12] introduced a framework for conducting rule-based compliance tests for ISO/IEC 27001 controls. This framework utilizes ontological data to support the audit process by allowing for the visualization and reasoning of compliance data. Through the use of ontologies, auditors can gain a deeper understanding of the relationships between different security controls and identify areas where compliance gaps may exist.

To complement the NIST 800-30 risk management standard, the Automated Risk and Utility Management technique was developed in [13]. This technique models an organization's assets within an ontological framework, providing a structured approach to improving information security risk management. By integrating this framework with existing standards like ISO/IEC 27004, organizations can enhance their risk assessment processes and make more informed decisions regarding resource allocation and control implementation.

Several studies have also focused on the challenges faced by small and medium-sized enterprises (SMEs) in adopting ISO/IEC 27001 [14]. SMEs often lack the financial and technical resources required to fully implement an ISMS, and as a result, they face significant barriers to compliance. These studies highlight the need for tailored solutions that account for the specific constraints of SMEs, including simplified control sets and more cost-effective approaches to risk management.

In the study [15], the SHA-256 hash function was chosen to model an attack using rainbow tables, and the algorithm for constructing rainbow tables was implemented in the Cryptool 2 environment. During the study, the conditions were determined under which the use of rainbow tables would be most effective. The purpose of this study was a practical study of the process of password generation and creation of rainbow tables for organizing an attack on the SHA-256 hash function. Research confirms that the use of salt when hashing passwords significantly increases their security, which makes rainbow tables less effective. This aspect emphasizes the importance of using salt in authentication systems to improve the level of data security.

In response to the growing demand for security education, the Heuristic Preconditions Assistant was proposed in [16]. This strategy provides a framework for educating developers and designers on security best practices by modeling workflows and allowing stakeholders to share knowledge related to security requirements at the project level. By incorporating security into the early stages of development, organizations can reduce the likelihood of vulnerabilities being introduced into their systems.

A method for evaluating the security performance of SCADA networks was introduced in [17]. This study demonstrated the effectiveness of the ISO/IEC 27004 measurement standard when applied to Supervisory Control and Data Acquisition (SCADA) systems. SCADA networks are critical to the operation of many industrial control systems, and securing these networks is of paramount importance. The study emphasized the need for risk-based security controls that prioritize the most significant threats and vulnerabilities.

For the integration of ISO/IEC 27001 into an enterprise architecture, a business engineering technique was adopted in [18]. This approach divides the organization into four distinct layers:

Strategic Layer: Aligns internal and external organizational requirements with the organization's strategic goals.

Organizational Layer: Defines the overall process vision for the organization and assigns roles and responsibilities within the ISMS.

Information System Layer: Focuses on managing information assets and defining the information architecture, including software components and platforms.

Technological Layer: Deals with the technological infrastructure required to support the organization's security processes.

These layers help organizations implement ISO/IEC 27001 in a structured manner, ensuring that all aspects of the business are aligned with security objectives.

In article [19-20] proposes to consider the possibility of using Blockchain technology to create a new generation data protection system capable of providing both direct and indirect information security. An example of a possible system implementation model is given that takes into account both the logic of direct data encryption and the analysis of the entire chain of interactions with data, including past and future operations. The applicability of this approach to ensuring data security both in corporate systems and for individual users is shown.

This article [21] discusses methods for ensuring data security when using neural networks to predict environmental processes. It shows the importance of integrating robust security measures to protect sensitive environmental information and increase confidence in neural network-based predictions.

In the article [22] discusses ways to counteract illegal cryptocurrency mining, known as cryptojacking. The main focus is on identifying the characteristic signs and properties of cryptojacking, as well as modern methods for detecting this threat. Using the proposed indicators helps protect end systems from unauthorized use of their resources for mining. One of the important aspects of modern cybersecurity is the strength of hashed messages, which plays a key role in authentication systems.

In the study [23], the SHA-256 hash function was chosen to model an attack using rainbow tables, and the algorithm for constructing rainbow tables was implemented in the Cryptool 2 environment. During the study, the conditions were determined under which the use of rainbow tables would be most effective. The purpose of this study was a practical study of the process of password generation and creation of rainbow tables for organizing an attack on the SHA-256 hash function. Research confirms that the use of salt when hashing passwords significantly increases their security, which makes rainbow tables less effective. This aspect emphasizes the importance of using salt in authentication systems to improve the level of data security.

Modern networks face challenges with traditional Quality of Service (QoS) methods that may not be effective enough to monitor and analyze data in the face of growing cybersecurity threats. These methods often face limitations in accuracy and real-time processing of big data, which may expose the system to vulnerabilities. To improve the level of cybersecurity, it is necessary to use intelligent fault classification systems that can quickly and accurately detect and diagnose errors that occur during system operation.

In summary, the literature emphasizes the importance of developing balanced approaches to implementing, measuring, and evaluating cybersecurity controls based on best practices. While automation offers significant advantages in terms of operational efficiency, the need for skilled professionals to oversee and interpret the results of automated systems remains critical. The

integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity management is seen as a future direction, but further research is needed to ensure that these technologies can be effectively incorporated into established standards like ISO/IEC 27001 and ISO/IEC 27004.

3. Method and tools

Measurement Information Model The ISO/IEC 27001 standard requires organizations to continually evaluate the performance and effectiveness of their Information Security Management Systems (ISMS). This ongoing evaluation is essential to ensure that security controls are functioning as intended and that they align with the organization's overall security goals. At the core of this process is the establishment of Key Performance Indicators (KPIs), which serve as measurable metrics providing insights into how well an organization's security controls are implemented and their effectiveness in mitigating risks.

Defining Base Measures

The first step in developing a comprehensive security assessment system is to define base measures. These base measures represent fundamental metrics that reflect specific aspects of information security. For example, metrics might include the total number of security incidents, the time taken to resolve them, or the number of vulnerabilities identified over a specific period.

Each base measure provides a detailed understanding of a particular security process. For instance:

$$BM_1 = Numberof\ Incidents\ BM_2 = ¿\ \text{Average Resolution Time} \quad (1)$$

Where:

- BM_1represents the number of incidents recorded within a given time frame;
- BM_2 represents the average time taken to resolve each incident.

By collecting and analyzing these base measures, organizations can construct a detailed picture of their security posture. The use of multiple base measures enables a more granular and specific evaluation of different areas of cybersecurity.

Measurement Function

Once the base measures are defined, the next step involves applying a measurement function to combine these base metrics into a more comprehensive derived measure. The derived measure provides deeper insight into the organization's overall performance by integrating multiple base measures. This can be achieved using a variety of mathematical functions, such as ratios, percentages, or more complex formulas.

For example, one common measurement function might assess the ratio of security incidents to the time taken to resolve them. This can be represented as:

$$DM = f\left(BM_1 BM_2\right) = \frac{BM_1}{BM_2} \quad (2)$$

Where:

- BM_1: number of security incidents;
- BM_2: average response time to resolve incidents;
- DM - the derived measure, representing the ratio of incidents to response time, which serves as an indicator of the organization's incident management effectiveness.

Derived measures can be used to identify trends and patterns in security performance, helping organizations pinpoint areas where improvements are needed.

Interpreting Derived Measures

Once the derived measures are calculated, they must be interpreted in the context of the organization's broader security goals. This process involves comparing the derived metrics against predefined benchmarks or thresholds to determine whether performance is meeting expectations.

For example, organizations might set target values for certain metrics, such as resolving 90% of incidents within 48 hours. If the derived measure falls short of this benchmark, this may indicate a need for process optimization or additional resources.

This comparison can be represented mathematically as:

$$\Delta = \frac{DM_{actual} - DM_{target}}{DM_{target}} \times 100 \quad (3)$$

Where:

- DM_{actual} is the actual derived measure;
- DM_{target} is the target derived measure;
- Δ is the percentage deviation from the target.

This formula provides a clear indication of whether the organization is meeting its security goals or if corrective actions are needed.

Generating Information Products

The final step in the measurement process is the creation of information products, which are the reports, dashboards, or data visualizations generated from the analysis of the derived measures. These information products allow decision-makers to interpret the results of the security assessment in a clear and actionable manner. For example, a dashboard might present key metrics, such as incident resolution times, in a visual format (e.g., graphs or charts), enabling quick identification of trends and areas of concern.

The use of dashboards and automated reports helps simplify the interpretation process and ensures that key stakeholders are informed about the organization's security performance. By transforming raw data into meaningful insights, these information products support strategic decision-making and help organizations maintain a strong security posture.

Holistic View and Extended Analysis

A holistic approach to cybersecurity measurement is essential for gaining a comprehensive understanding of an organization's security landscape. Such an approach involves considering both quantitative and qualitative factors. Quantitative metrics, such as the number of incidents or average resolution time, provide important data on the organization's ability to respond to threats. However, qualitative factors such as the complexity of the incidents or the severity of vulnerabilities—are equally important in providing context and guiding decision-making.

For example, an organization might track the trend of security incidents over time using the following formula:

$$T_{trend} = \frac{S_{current - S_{previous}}}{S_{previous}} \times 100 \quad (4)$$

Where:

- $S_{current}$is the number of incidents in the current period;
- $S_{previous}$ is the number of incidents in the previous period.

This formula provides the percentage change in the number of incidents, allowing the organization to assess whether its security posture is improving or deteriorating over time. An upward trend may signal that additional controls or resources are needed to address an increasing number of incidents, while a downward trend may suggest that current security measures are effective

Qualitative analysis complements this by examining factors such as the severity of each incident, the resources required to mitigate them, and any potential lessons learned. This holistic view ensures that the organization not only responds to threats in a timely manner but also continuously improves its security processes.

Standardization of Metrics

To ensure that the results of different metrics can be compared and interpreted consistently, organizations often employ standardization techniques. Standardization allows metrics measured on different scales or with different units to be transformed into comparable values. This process is particularly important when analyzing a diverse set of metrics, such as those related to incident response times, vulnerability management, or system uptime.

One common method of standardization involves transforming raw data into z-scores, which represent the number of standard deviations a data point is from the mean. The formula for calculating the z-score is:

$$z = \frac{x - u}{s} \tag{5}$$

Where

- z is the new value;
- x is the original value;
- u is the mean and s is the standard deviation.

By using z-scores, organizations can compare metrics that may otherwise be difficult to evaluate side by side. For example, z-scores can be used to compare the effectiveness of different security controls, even if the controls are measured using different units or scales.

The standard deviation is a measure of how evenly distributed the numbers are (2). Most of the data are likely close to the mean (average) value if the standard deviation is low. When the standard deviation is large, it indicates that the values are spread out over a wider range, meaning the data points are more dispersed from the mean. The formula for calculating standard deviation is:

$$\sigma = \sqrt{\frac{\sum (x_i - \mu)^2}{N}} \tag{6}$$

Where

- N - the size of the population,
- xi each value from the population
- μ is the population mean.
- σ is the standard deviation,

Measurements analysis on the ISO/IEC 27004 example

The metrics defined in this study adhere closely to the principles laid out in the ISO/IEC 27004 standard, which provides a structured framework for evaluating the effectiveness of an organization's Information Security Management System (ISMS). By linking each metric to specific control objectives within ISO/IEC 27001, the analysis ensures that the metrics are both globally standardized and relevant to real-world security practices. In total, 35 distinct metrics were analyzed, covering various aspects of security management.

These metrics vary significantly in terms of the input data required, measurement formulas used, the frequency of data collection, and the overall complexity of analysis. For instance, some metrics involve simple ratios, while others require complex mathematical formulas to evaluate performance over time.

Categorization of Metrics

To facilitate better understanding and comparison, the metrics were categorized based on their measurement functions. Table [1] below presents the distribution of metrics according to the type of measurement function applied.

Table 1
Various Measurement Approaches

Measurement Function/Formula	Number of Metrics
Ratio	1
Percentage	9
Complex Ratio/Percentage	5
Average/Trend	5
Sum	3
Multiplication	1
Scale	1

This categorization reveals that most metrics are calculated using ratios and percentages, reflecting their frequent use in evaluating security effectiveness. For instance, ratios are often used to express relationships between incidents and responses, while percentages can be useful for comparing successful threat mitigation rates relative to total attacks.

The majority of the metrics analyzed utilize ratios and percentages, reflecting their frequent use in security effectiveness evaluations. For example, ratios are commonly used to express relationships between security incidents and response times, while percentages provide a useful way to measure the success rate of threat mitigations relative to the total number of incidents.

Detailed Example of a Ratio-Based Metric

A key example of a ratio-based metric is the calculation of the Incident Resolution Effectiveness. This metric compares the number of incidents resolved within a specified time frame to the total number of incidents:

$$R_{effectiveness} = \frac{N_{resolvd}}{N_{total}} \times 100 \tag{7}$$

Where

- $R_{effectiveness}$ is the ratio of resolved incidents to total incidents;
- $N_{resolved}$ is the number of incidents resolved within the defined time frame;
- $N_{total}$is the total number of incidents.

This formula provides an easily interpretable percentage value, representing how effectively the organization is handling security incidents. If the value is close to 100%, it indicates that most incidents are being resolved promptly, which is a positive indicator of the organization's incident management performance.

Complex Metrics: Combining Multiple Factors

Some metrics require more complex calculations, as they combine multiple base measures into a single derived metric. An example of this is the calculation of security incident trends, which looks at both the frequency of incidents and the time taken to resolve them. The formula for calculating this trend might involve the following:

$$T_{trend} = \frac{S_{current} - S_{previous}}{S_{previous}} \times 100 \tag{8}$$

Where

- T_{trend} is the percentage change in incidents over a specific time period;
- $S_{current}$is the number of incidents in the current period;
- $S_{previous}$ is the number of incidents in the previous period.

This metric provides insight into whether the number of security incidents is increasing or decreasing, allowing organizations to adjust their security measures accordingly.

4. Analysis of results and their interpretation

Once the metrics were calculated, the results were carefully analyzed and interpreted in relation to the organization's cybersecurity goals. Table [2] below presents the actual values of some of the key metrics calculated during the study.

Table 2
Evaluated Results

Metric	Actual Value
Security Incidents Trend	0.86
Information Security Incident Management	0,68
Physical Entry Controls Effectiveness	1,027
Learning from Information Security Incidents	0,82
Protection Against Malicious Code	0,89

The results presented in Table [2] reflect the performance of the organization in several critical areas. For example, the Security Incidents Trend metric shows a positive trend (0.86), indicating that the number of incidents is decreasing over time. This suggests that the organization's current security measures are having a positive impact.

On the other hand, the Physical Entry Controls Effectiveness metric (1.027) highlights a critical weakness in the organization's physical security processes. This high value indicates that the physical security controls are not as effective as expected, signaling the need for improvement.

5. Interpreting the color indicators

To aid in the interpretation of these results, color-coded indicators were used. These indicators provide a quick and intuitive way to assess whether the organization's performance in a particular area is satisfactory (green), requires attention (yellow), or is in critical need of improvement (red).

For instance:

A Green indicator signifies that the organization is meeting or exceeding its cybersecurity goals in that area.

A Yellow indicator suggests that the organization's performance is below expectations and may require further attention or resources.

A Red indicator signals that immediate action is needed to address a significant weakness in the organization's security controls.

The detailed analysis of metrics based on the ISO/IEC 27004 standard provides valuable insights into an organization's cybersecurity performance. By using a combination of simple and complex metrics, organizations can gain a comprehensive view of their security posture. This allows decision-makers to take proactive steps to improve security processes and allocate resources more effectively.

Future research will focus on refining these metrics and developing more sophisticated models for evaluating security effectiveness. In particular, integrating machine learning algorithms and predictive analytics into cybersecurity measurement models holds great potential for enhancing the accuracy and timeliness of security assessments.

6. Results and discussion

This section provides an in-depth analysis of the key security metrics for the organization, focusing on trends, incident types, and the effectiveness of control measures. The discussion is based on the data collected from 2019 to 2024, with particular emphasis on the years 2022 to 2024. The following subsections will explore key insights drawn from the data.

6.1 Security incidents trend

The analysis of the Security Incidents Trend from 2022 to 2024 highlights a consistent decline in the number of security incidents, reflecting improvements in the organization's cybersecurity measures. The incidents are recorded and analyzed quarterly, and the trend is visualized in Figure 1, which shows the steady reduction in the number of incidents.

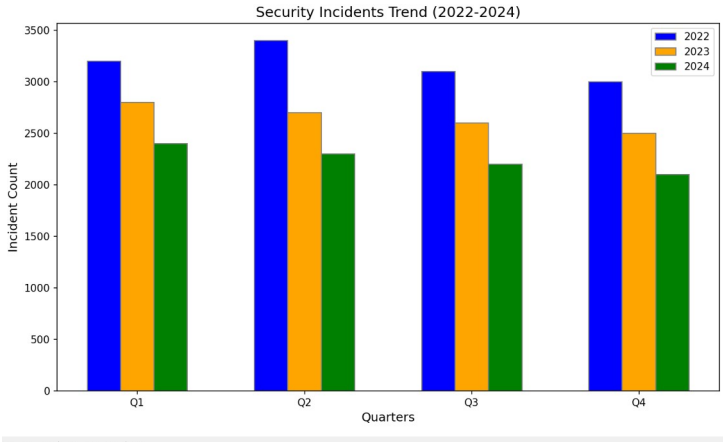

Figure 1: Security Incidents Trend from 2022 to 2024.

As illustrated in Figure [1], the incident counts decreased steadily across quarters for each year. For example, in 2022, the number of incidents was highest in Q2 but began to drop in Q3 and Q4. This trend continued into 2023, with a further decrease in the overall number of incidents in each quarter. By 2024, the incident count had significantly reduced, showing a continued improvement in the organization's security posture.

6.2 Unauthorized access incidents (2022-2024)

Unauthorized access incidents, one of the most significant security threats, were carefully monitored throughout the analyzed period. These incidents involved unauthorized attempts to gain access to sensitive systems and data, and they pose a critical threat to the organization's overall cybersecurity posture. As shown in Figure 2, the number of unauthorized access incidents peaked in Q2 of 2022 but began to decline steadily after that. This trend reflects the organization's strategic implementation of advanced security measures, such as Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and stricter password policies.

Key Findings:

1. **Peak in Early 2022:**

Unauthorized access incidents spiked in the first half of 2022 due to an increased volume of targeted phishing and credential stuffing attacks. Attackers exploited weak credentials and insufficient authentication mechanisms to gain access to critical systems.

2. **Decline Starting Q3 2022:**

The introduction of MFA and more stringent access control measures in mid-2022 led to a significant reduction in the number of unauthorized access incidents by Q3 of the same year. These measures

added an additional layer of security, making it more difficult for attackers to bypass authentication systems.

3. **Continued Improvement in 2023 and 2024:**

By 2023, unauthorized access incidents had decreased significantly. The adoption of behavioral analytics and real-time monitoring tools further mitigated unauthorized access attempts. By the end of 2024, the trend had stabilized, indicating the sustained effectiveness of the implemented controls.

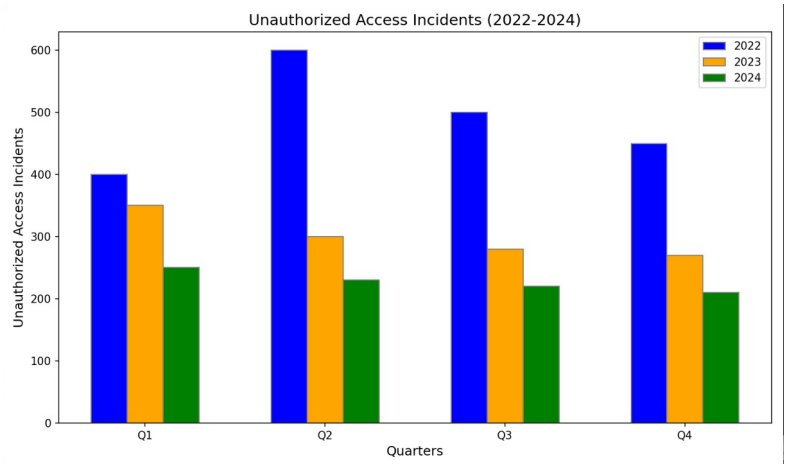

Figure 2: Unauthorized Access Incidents (2022-2024.

The analysis of Unauthorized Access Incidents from 2022 to 2024 reveals significant progress in reducing the frequency of such incidents. The data shows that unauthorized access attempts peaked in early 2022 but steadily declined by the end of 2024. This downward trend can be attributed to several critical security measures, including the implementation of Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and continuous monitoring of user behavior through advanced security analytics.

Key improvements such as the integration of automated access control systems, regular audits, and improved user awareness played pivotal roles in minimizing unauthorized access attempts. The organization's proactive approach to bolstering both technical and physical security resulted in a significant reduction in incidents, demonstrating the effectiveness of a comprehensive security strategy.

The introduction of Zero Trust Architecture in mid-2023 further strengthened defenses, as it required continuous verification of user identities and access privileges. This approach helped to mitigate risks associated with insider threats and credential-based attacks.

In conclusion, the organization's focus on strengthening access control mechanisms and enhancing incident response procedures led to measurable improvements in mitigating unauthorized access incidents. Continued investments in security automation, employee training, and periodic audits will be critical to maintaining these positive outcomes and ensuring long-term protection against evolving threats.

The analysis of unauthorized access incidents from 2022 to 2024 reveals a positive trend in reducing security threats related to unauthorized access attempts. The peak in early 2022, primarily driven by credential-based attacks and phishing attempts, was effectively addressed through the implementation of advanced access control measures. The introduction of Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Zero Trust Architecture significantly contributed to reducing the number of incidents by mid-2023.

Furthermore, continuous investments in real-time monitoring and behavior analytics played a pivotal role in detecting and preventing unauthorized access attempts. By 2024, the organization achieved a more stable and controlled security environment, with a marked reduction in the frequency of unauthorized access incidents.

The integration of technical controls with improved user awareness and regular security audits also strengthened the organization's security posture. The downward trend observed over this period highlights the success of a holistic and adaptive approach to access control management.

6.3 Incident resolution times (2022-2024)

Incident resolution times are a critical metric in evaluating the effectiveness of an organization's response to security breaches. Shorter resolution times typically indicate a more effective and responsive incident management process. By minimizing the time it takes to detect, investigate, and resolve security incidents, organizations can reduce the potential damage caused by these incidents and prevent further escalation.

Key Findings

The analysis of Incident Resolution Times from 2022 to 2024 shows significant improvements across the analyzed period. The data is broken down into four categories based on the time taken to resolve incidents: Less than 24 hours; 24 to 72 hours; 72 hours to 1 week; More than 1 week

The trends over this period, visualized in Figure 3, indicate that the number of incidents resolved within 24 to 72 hours significantly increased from 2022 to 2024, while incidents taking more than 1 week to resolve saw a steady decrease.

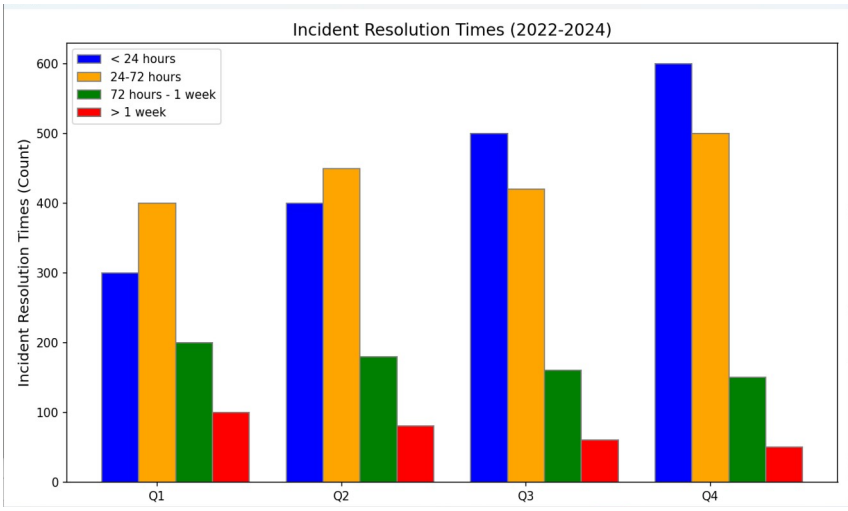

Figure 3: Incident Resolution Times (2022-2024).

7. Analysis of improvements

Faster Detection and Response: The introduction of automated incident detection tools, such as Security Information and Event Management (SIEM) systems, enabled the organization to detect and respond to incidents more swiftly. These tools allowed for real-time monitoring, which contributed to the reduction in incidents taking more than 72 hours to resolve.

Streamlined Incident Management Procedures: The organization revised its incident management workflow, reducing administrative overhead and ensuring that incidents were escalated and addressed promptly. By improving communication and coordination between teams, incidents were resolved more efficiently, especially those in the 24 to 72-hour window.

Continuous Incident Response Training: Regular training sessions for the incident response team helped sharpen their skills in handling security breaches. These trainings, combined with regular incident drills, ensured that the team could respond quickly and effectively in real-world scenarios. This contributed to a noticeable reduction in the number of incidents that took more than 1 week to resolve.

Increased Automation in Remediation Processes: Automation played a key role in accelerating incident resolution times, particularly in repetitive tasks such as patching vulnerabilities and

isolating affected systems. The use of automated response mechanisms ensured that known threats were dealt with swiftly, minimizing the time required for manual intervention.

The decrease in incident resolution times from 2022 to 2024 is a clear indication of the organization's improved incident management capabilities. In 2022, the organization faced challenges in resolving incidents in a timely manner, with a significant number of incidents taking more than 1 week to resolve. However, by the end of 2024, the majority of incidents were resolved within 72 hours, demonstrating the effectiveness of the measures implemented during this period.

One of the standout improvements was the shift toward resolving incidents in less than 72 hours. This rapid resolution was made possible by a combination of real-time threat detection, streamlined incident handling processes, and the application of automated tools for response and remediation. Moreover, the organization's focus on continuous training and preparedness ensured that the incident response team was capable of managing complex threats with speed and precision.

The analysis of key security metrics from 2022 to 2024 provides valuable insights into the organization's evolving cybersecurity posture. The Security Incidents Trend demonstrates a significant reduction in the number of incidents over the analyzed period, reflecting the organization's proactive efforts in strengthening its cybersecurity measures. The decline in incidents is largely attributed to the successful implementation of advanced security controls, including Multi-Factor Authentication (MFA) and continuous monitoring tools.

Similarly, the data for Unauthorized Access Incidents shows a marked improvement, with the number of incidents decreasing steadily across the years. This outcome highlights the effectiveness of access control measures, such as Role-Based Access Control (RBAC) and the introduction of Zero Trust Architecture, in mitigating unauthorized access attempts.

The analysis of Incident Resolution Times revealed a consistent improvement in how quickly security incidents were addressed. Most incidents were resolved within 72 hours, with the number of incidents taking more than one week to resolve dropping significantly. This improvement is a result of enhanced incident response capabilities, the adoption of automated tools, and regular incident response training.

Overall, the data shows that the organization has made significant progress in improving its cybersecurity defenses. However, continued focus on refining incident response processes, adopting emerging security technologies, and ongoing staff training will be essential to maintain and further strengthen this positive trend.

The analysis of incident resolution times from 2022 to 2024 demonstrates a significant improvement in the organization's ability to resolve security incidents efficiently. The number of incidents resolved within the critical 24 to 72-hour window increased substantially, reflecting enhancements in the incident response process and the effective use of automation in remediation.

The combination of Security Information and Event Management (SIEM) systems, real-time detection tools, and streamlined communication among response teams contributed to a notable decrease in incidents taking more than one week to resolve. Additionally, continuous incident response training and the automation of routine tasks, such as vulnerability patching, further reduced manual intervention time.

Overall, the organization's focus on optimizing its incident management workflow, coupled with investments in both technology and personnel training, has proven to be highly effective. This improvement in incident resolution times showcases the organization's capability to handle security incidents swiftly and mitigate potential risks before they escalate.

8. Conclusion

This study assessed the organization's cybersecurity performance from 2022 to 2024, focusing on the Security Incidents Trend, Unauthorized Access Incidents, and Incident Resolution Times. The analysis reveals significant advancements in the organization's ability to detect, respond to, and mitigate security incidents.

One of the most notable findings is the substantial reduction in overall security incidents, particularly unauthorized access attempts. This improvement reflects the organization's commitment to investing in modern security technologies and enhancing its incident response procedures. The adoption of comprehensive security measures, such as Multi-Factor Authentication (MFA), Zero Trust Architecture, and Role-Based Access Control (RBAC), has been instrumental in achieving these outcomes.

Additionally, the organization demonstrated improvements in incident resolution times, with most incidents being resolved within 72 hours. The effective use of Security Information and Event Management (SIEM) systems, real-time monitoring, and regular incident response training played a critical role in reducing resolution times.

Moving forward, the organization should continue to prioritize investments in advanced security technologies and processes. Continuous monitoring and improvement of security measures will be vital in addressing emerging threats and ensuring long-term resilience. Furthermore, staff training and awareness programs should be maintained to ensure that the human element remains a strong line of defense against cyber threats.

In conclusion, the organization has made significant strides in improving its cybersecurity posture from 2022 to 2024, but maintaining this progress will require ongoing efforts and adaptability in the face of evolving cyber threats.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Accenture Insights "Why you need to capitalize on the rise of the data-driven enterprise", 2021.

[2] ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection - Information security management systems – Requirements".

[3] ISO/IEC 27004:2016 "Information technology — Security techniques — Information security management — Monitoring, measurement, analysis, and evaluation".

[4] R. Montesino and S. Fenz, "Automation possibilities in information security management," in European Intelligence and Security Informatics Conference. Athens, Greece: IEEE, 2011, pp. 259–262.

[5] K. Hajdarevic, C. Pattinson, K. Kozaric, A. Hadzic " Information Security Measurement Infrastructure for KPI Visualization" MIPRO, 2012/ISS.

[6] A. P. Aldya, S. Sutikno, Y. Rosmansyah "Materials Science and Engineering:2018 Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004:2013 standard" IOP Conference.

[7] W. Boehmer"Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001" IInd International Conference on Emerging Security Information, Systems and Technologies,2008.

[8] F. Enayaty-Ahangara , L. A. Albertb , and E. DuBois "A survey of optimization models and methods for cyberinfrastructure security" IISE TRANSACTIONS, 2020.

[9] S. E. Chang and C. B. Ho, "Organizational factors to the effectiveness of implementing information security management," Industrial Management & Data Systems, vol. 106, no. 3, 2006, pp. 345–361.

[10] D. Mellado, E. Fernandez-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," Computer Standards & Interfaces, vol. 29, 2007.

[11] M. M. Anwar, M. F. Zafar, and Z. Ahmed, "A proposed preventive information security system," 2007 International Conference on Electrical Engineering. Lahore, Pakistan: IEEE, 2007.

[12] S. Fenz, "Ontology-based generation of IT-Security metrics," in ACM Symposium on Applied Computing. Sierre, Switzerland: ACM, 2010.

[13] A. Ekelhart, S. Fenz, and T. Neubauer, “AURUM: a framework for information security risk management,” 42nd Hawaii International Conference on System Sciences. Big Island, HI, USA: IEEE, 2009.
[14] T. Valdevit and N. Mayer, “A gap analysis tool for smes targeting ISO/IEC 27001 compliance,” 12th International Conference on Enterprise Information Systems, Funchal, Madeira - Portugal, 2010.
[15] Babenko, Tetiana, Kolesnikova, Kateryna, Lisnevskyi, Rostyslav,Makilenov, Shakirt,Landovsky Yuriy Definition of Cryptojacking Indicators CEUR Workshop Proceedings Volume 36802024 8th International Conference on Digital Technologies in Education, Science and Industry, DTESI 2023Almaty6 December 2023through 7 December 2023.
[16] K. Schneider, E. Knauss, S. H. Houmb, S. Islam, and J. Jurjens, “Enhancing security requirements engineering by organisational learning,” Requirements Engineering, vol. 17, no. 1, 2012.
[17] M. P. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, “A propose technical security metrics model for SCADA systems,” International Conference on Cyber Security, Cyber Warfare and Digital Forensic. Kuala Lumpur, Malaysia: IEEE, 2012.
[18] V. Hensel and K. Lemke-Rust, “On an integration of an information security management system into an enterprise architecture,” International Workshop on Database and Expert Systems Applications. Bilbao, Spain: IEEE, 2010.
[19] Kateryna Kolesnikova, Rostyslav Lisnevskyi, Lukyanov Dmitry. Using Blockchain Technology In Scientometrics. 8 International Conference on Digital Technologies in Education, Science and Industry (DTESI 2023) https://ceur-ws.org/Vol-3680/Short4.pdf.
[20] Hladkyi, M. Gladka, M. Kostikov, R. Lisnevskyi, An IoT Solution: A Fitness Trainer, in: CEUR Workshop Proceedings, 2021, 3179, pp. 215–226.
[21] ISO/IEC/IEEE 15939:2017 Systems and software engineering — Measurement process Guidance on AI and data protection, https://ico.org.uk/.
[22] Manankova, O.A., Yakubova, M.Z., Rakhmatullaev, M.A., Baikenov SIMULATION OF THE RAINBOW ATTACK ON THE SHA-256 HASH FUNCTION A.S.Journal of Theoretical and Applied Information Technology, 2023, 101(4), pp 1594–1603.