# MODERN APPROACHES TO PROTECTIVE MEASURES IN CORPORATE SECURITY

**Hadžib SALKIĆ**
**Nedžad KORAJLIĆ**
**Dušan RAJČEVIĆ**

***Abstract:*** *In the era of digital transformation, data security has emerged as a paramount challenge for corporations worldwide, particularly in the context of increasingly sophisticated cyber-attacks. This study examines the efficacy of security measures within corporate environments, with a focus on mitigating prevalent cyber-attacks such as phishing, malware infection, distributed denial-of-service (DDoS) attacks, ransomware and SQL injection. By analyzing empirical data from 50 enterprises in Bosnia and Herzegovina, the research evaluates three critical dimensions, the extent of security protocol implementation, the risk-reduction impact of adopting ISO/IEC 27001 compliance, and the comparative effectiveness of paid versus free security software in safeguarding business infrastructure. Utilizing Pearson, Spearman and Kendall correlation analyses, the findings reveal that organizations employing integrated measures (firewall, encryption, regular audits) and paid tools such as endpoint protection, exhibit a statistically significantly reduction in successful cyber-attacks ($p < 0.05$) compared to those that rely on free or built-in security features of operating systems. The study highlights the necessity of hybrid frameworks that integrate advanced technological solutions, adherence to international standards and ongoing staff training. The study contributes a novel regional perspective, addressing the unique challenges of cyber security faced by organizations in resource-limited settings.*
***Keywords:*** *cyber security, data security, phishing, ransomware, DDos, SQL injection*

## 1. INTRODUCTION

Digitalization of business operations and the increasing use of information technologies bring numerous advantages but at the same time increase the risk of cyber-attacks. Corporations are faced with challenges in protecting sensitive data and maintaining the security of their information systems. Considering the diverse threats, from phishing attacks and ransomware to distributed denial-of-service (DDoS) attacks and SQL injections, the question arises as to which security measures are most effective in preventing these threats. This paper examines modern approaches to data protection in corporate security, analyzing the implementation of security measures in Bosnian and Herzegovinian companies. Particular focus is placed on analyzing the differences between companies that use free security tools and those that invest in commercial solutions. The aim of the research is to identify which security measures yield the best results in preventing cyber-attacks and to determine how the application of ISO standards contributes to

the security of business systems. In addition to descriptive data analysis, the study employs statistical methods, including Pearson, Spearman, and Kendall correlation, to establish relationships between different security approaches. Based on these analyses, the paper provides recommendations for improving corporate security through the implementation of advanced security measures and a combination of free and paid solutions.

## 2. METHODOLOGY

The research was conducted on a sample of 50 companies in Bosnia and Herzegovina across various industrial sectors, including IT, finance, manufacturing, and retail. The sample was formed using a targeted selection method, including companies that process and store sensitive data. Data was collected through structured surveys and interviews with IT managers and information security experts.

The results show the following distribution in the application of data protection measures:

- 34% (17 companies) apply all data protection measures.
- 48% (24 companies) partially apply data protection measures.
- 18% (9 companies) do not apply any data protection measures.

To determine the factors influencing the level of implementation of security measures, statistical analysis was conducted using Pearson, Spearman, and Kendall correlations. The following relationships were analyzed:

- The link between investment in security tools (free vs. paid software) and the level of data protection.
- The correlation between company size and the frequency of security audits.
- The relationship between the frequency of employee training and the level of protection from cyber threats.

Based on these analyses, the paper provides recommendations for optimizing corporate security through more efficient implementation of protective measures, as well as a combination of free and paid security solutions.

## 3. DATA PROTECTION MEASURES

### 3.1. Most Commonly Used Data Protection Measures

To reduce the risk of unauthorized access and misuse of data, organizations implement various protection measures. Among the most commonly used measures are:

**Pseudonymization and Encryption:** These techniques significantly reduce the risk of unauthorized access to personal data. Pseudonymization involves processing data in a way that it cannot be linked to a specific individual without additional information that is stored separately, while encryption converts data into an unreadable format that can only be decrypted using the appropriate key.

**Tokenization:** This method replaces sensitive data with non-sensitive tokens, that can be used for data processing without revealing the actual values.

Tokenization is especially useful in the financial sector and during payment card processing.

**Organizational Policies and Procedures:** Clearly defined rules and policies regarding the processing and protection of personal data ensure consistent application of security measures within the organization. Examples include internal regulations on data access, record-keeping, and procedures for reporting security incidents.

### 3.2. Measures that are partially implemented

Some data protection measures are not consistently implemented across all organizations, which can increase the risk of cyber-attacks. Among them are:

**Employee Training:** Although training is crucial for the proper implementation of security measures, it is often applied sporadically or is not mandatory for all employees. Employees who are not familiar with risks and protection practices may inadvertently compromise data security.

**Regular Security Audits:** Security checks are essential for identifying vulnerabilities in systems and procedures, but some companies do not conduct them regularly or do them superficially, without detailed analysis of the results and recommendations for improvements.

**Software and System Updates:** Although software updates are critical for security, some companies perform them irregularly, which can leave systems vulnerable.

### 3.3. Measures that are rarely or never implemented

Certain advanced security measures are highly effective but are rarely used due to high costs, complexity of implementation, or a lack of skilled personnel.

**Advanced Protection Techniques:** These include advanced encryption methods, multi-factor authentication (MFA), biometric verification, and quantum cryptography. Although they significantly enhance security, many companies avoid them due to high technical requirements and implementation costs.

**Incident Response Plans:** Organizations often lack formalized plans for responding to cyber-attacks. Without defined procedures, the response time to attacks may be prolonged, increasing the damage to the organization and its clients.

**Continuous Education:** Regular employee training on new threats and security practices is often neglected. Cyber threats are constantly evolving, requiring continuous adaptation and enhancement of employees' knowledge to protect the organization from new types of attacks.

### 3.4. Impact of Protection Measures on the Probability of Cyber-Attacks

Quantitative analysis of the impact of protective measures on the risk of cyber-attacks encompassed two aspects:

1. Implementation of the ISO/IEC 27001 standard, and
2. Efficiency of different levels of technical data protection (basic, intermediate, advanced).

In Table 1, we present the data on the frequency of cyber-attacks in organizations with certified ISO standards compared to non-certified ones, while on Fig. 1, using blue bars, we visually display the negative correlation between the implementation of standards and attack rates.

Results show that companies with full implementation of ISO/IEC 27001 report a 30–60% lower attack rate, with the greatest reduction observed in phishing and ransomware incidents.

*Table 1. Probability of Cyber-attacks – ISO standards*

| Category | Probability of *Cyber* Attack |
|---|---|
| **All ISO standards** | 0.1 |
| **Some ISO standards** | 0.4 |
| **Without ISO standards** | 0.7 |

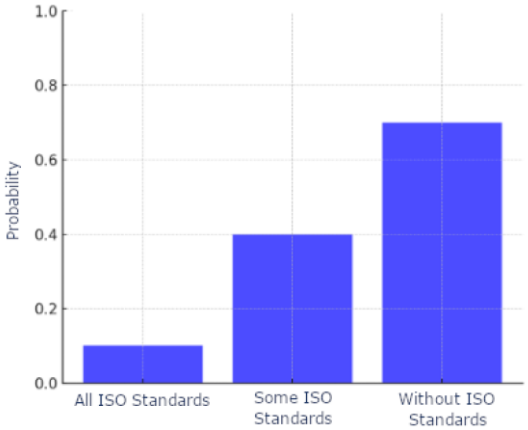


*Fig. 1 Probability of Cyber-attacks – ISO Standards*

In Table 2, we summarize the data on the likelihood of attacks based on the application of specific technical measures (e.g., multi-factor authentication, network segmentation, IDS/IPS systems) while on Fig. 2 we visually display the strong linear and nonlinear correlations between the number of implemented protective layers and the reduction of successful attacks. Organizations with the most advanced protection profiles (e.g., a combination of end-to-end encryption, regular automatic updates, and attack simulations) had up to 60% lower probability of system compromise compared to those with basic protocols.

*Table 2. Probability of Cyber-attacks – Security Measures*

| Category | Probability of Cyber Attack |
|---|---|
| **All security measures** | 0.15 |
| **Some security measures** | 0.5 |
| **Without security measures** | 0.85 |

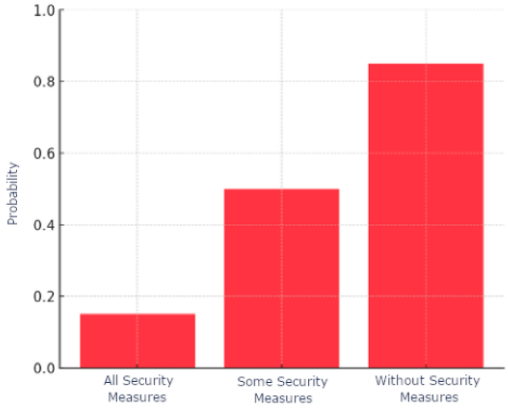


*Fig. 2 Probability of Cyber-attacks – Security Measures*

The key finding reflects the synergy between ISO standards and technical measures. Companies that combine ISO/IEC 27001 with multilayered protection achieve a 30-60% risk reduction, confirming the necessity of a holistic approach. This data further emphasizes that even minimal investment in upgrading protection (e.g., transitioning from basic to intermediate levels) lead to statistically significant improvements ($p < 0.05$).

While a significant number of companies in Bosnia and Herzegovina recognize the importance of data protection, there is room for improvement, particularly in the consistent application and updating of security measures. Companies should strive for full implementation of recommended measures to ensure adequate data protection and compliance with relevant legislation. (Salkić, H., Korajlić, N., Zajmović, M.2025)

### 3.5. Types of Cyber-Attacks on Companies

In Table 3, we present a classification of the analyzed cyber-attacks by type, target, methodology, and affected infrastructure. The table summarizes four dominant types of cyber-attacks identified in the research, along with their characteristics and impact on corporate infrastructure.

*Table 3. Types of Cyber-attacks on corporations*

| Type of attack | Goal of attack | Method of attack | Targeted infrastructure |
|---|---|---|---|
| **Ransomware** | Data lock with ransom demand | Malicious software via links | Dana storage systems |
| **DDoS Attack** | Disabling service operation rada | Flooding the server with fake requests | Web servers and network infrastructure |
| **Insider Threat** | Internal information leakage | Malicious behavior of employees | Internal databases and documents |
| **SQL Injection** | Unathorized access to the database | Manipulation of SQL queries | Databases and applications |

### 3.6. Analysis of Average Security Risks

On Fig. 4, represented with purple bars, we provide an overview of the risk assessment for each type of attack categorized by priorities in specific context without the implementation of additional protective measures.

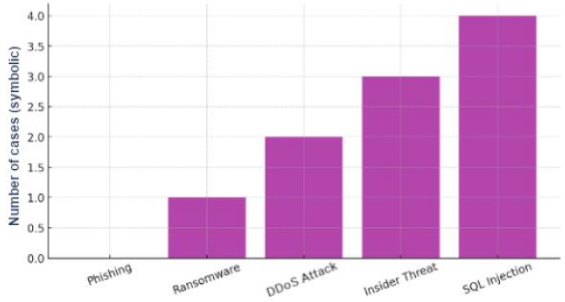


*Fig. 4 Most common types of cyber-attacks on corporations*

On Fig. 5, we show the same data, but taking into account improvements through security measures.

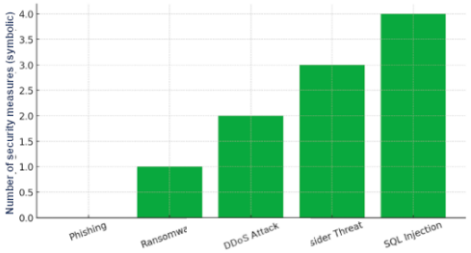


*Fig. 5 Security measures against cyber-attacks*

This shows that attack types such as SQL injection and DDoS remain high-risk even with additional protective measures, while less critical attacks, like phishing, show a significant reduction in assessed risk. This highlights the necessity for strategic management of security resources, focusing on attack types that have the greatest impact on the overall security landscape.

Three key types of cyber-attacks:

**Phishing attacks** rely on human error (Threatcop 2022), where attackers use fraudulent communication to obtain sensitive information. Recommended basic systemic security measures include multi-factor authentication (MFA) and email filtering (Clean Email 2025). Equipping employees (Hook Security 2023) with the skills to identify deceptive tactics and conducting simulated phishing exercises are essential for improving organizational resilience.

**Ransomware attacks** target the locking of organizational data, with a ransom demand. Regular creation of data backups and endpoint protection constitute basic preventive measures (Datto 2024). Additional measures include encryption of sensitive data and the use of isolated systems for backups (Hornetsecurity 2023) to minimize potential data loss in case of an attack.

**DDoS attacks (Distributed Denial of Service)** disrupt the availability of network resources by overloading systems with malicious traffic. (Cloudflare

2024) Firewalls, CDN protection, and load balancing represent essential systemic security measures. (Huawei Cloud 2025) Additionally, geolocation-based IP blocks and rate limiting provide more precise control and reduce network load during attacks. (IP2Location 2024)

The importance of combining systemic and additional protective measures in combating various forms of cyber threats is emphasized. While statistical data on the effectiveness of free and paid security solutions is not fully available, strategic planning and implementation of the mentioned measures significantly contribute to improving organizations' security posture.

### 3.7. Strategy for Protection Against Cyber-Attacks

**Phishing (Desolda, Ferro 2022):**

- **Employee education:** Regular training on recognizing suspicious emails, attachments, and links to reduce the likelihood of human error.
- **Antivirus software:** Using up-to-date antivirus programs that can detect and block malicious activities.
- **Spam filters:** Implementing sophisticated email filters to identify and automatically block phishing attempts.

**Ransomware (Salahdine, El Mrabet, Kaabouch 2021):**

- **Regular backups:** Creating and securely storing backups of critical data to ensure recovery in case of an attack.
- **Software updates:** Timely updates of operating systems and applications to patch known vulnerabilities that attackers might exploit.
- **Endpoint protection:** Implementing security solutions that protect network endpoints, such as workstations and mobile devices.

**DDoS Attacks (Bhuvana, Bhat, Shetty 2021):**

- **Network firewalls:** Using advanced firewalls capable of detecting and blocking malicious network traffic.
- **CDN services:** Applying Content Delivery Networks to help absorb increased traffic during attacks.
- **Load balancing:** Distributing network traffic to ensure optimal server load and prevent overloading.

**Insider Threats:**

- **Access control (LevelBlue 2024):** Limiting access to sensitive data exclusively to authorized individuals, following the "principle of least privilege."
- **Activity monitoring (Teramind 2025):** Introducing systems for continuous monitoring and analysis of user activities to detect unauthorized behavior.
- **Security policies (Fortinet 2025):** Establishing clear and binding rules regarding security standards within the organization.

**SQL Injections**

- **Secure coding (OWASP 2025):** Applying best practices in secure coding to ensure protection against SQL injections.
- **Input validation (Vumetric 2025):** Thorough validation and sanitization of user input to eliminate the possibility of malicious queries.
- **Software updates (SentinelOne 2025):** Timely updates of databases and applications to ensure resilience against known vulnerabilities.
-

### 3.8. Prevention of cyber-attacks

Although free security tools are often effective in basic protection, paid solutions usually offer more advanced functionalities and better support. Organizations should assess their specific needs and risks to select appropriate security solutions.

In Fig. 6, represented by yellow bars, we visually present the frequency of incidents for seven key types of cyber threats. Among these, Advanced Persistent Threats (APT) and insider threats are the most common, while phishing and malware attacks are less frequently observed.

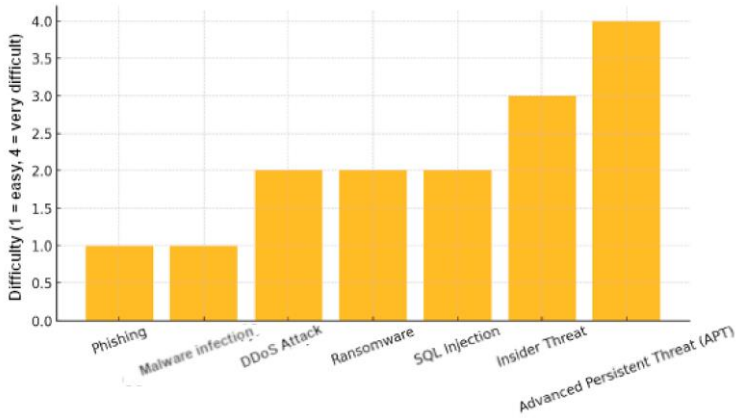


*Fig. 6 Difficulty of cyber-attack prevention*

**Ransomware:** Classified as moderately difficult to prevent. Key protective measures include regular creation of backups, implementation of data encryption, and the use of endpoint protection.

**SQL Injection:** Also identified as moderately complex to prevent. Validation of user inputs and regular updating of databases are essential for preventing these attacks.

**Insider Threats:** Due to their complexity, they fall into the category of difficult-to-prevent threats. Monitoring user activities and strict access control represent key strategies for minimizing risks.

**Advanced Persistent Threats (APT):** Identified as the most difficult to prevent due to their sophistication and long-term attack strategies. Advanced

security systems and integration of threat intelligence solutions are critical for detecting and preventing these attacks.

Combining this analysis indicates that the difficulty of prevention increases with the complexity of threats. At the same time, the recommended key protective measures provide guidelines for optimizing the security strategy, enabling organizations to focus their resources on the most critical areas.

An overview of recommended software solutions highlights tools that provide additional protection against specific types of cyber-attacks. Each tool is designed to specifically combat threats and supplement existing security measures implemented in organizations.

**Phishing:** Recommended tools such as Proofpoint, Mimecast, and Microsoft Defender for Office 365 focus on filtering malicious emails, protecting against fraudulent communications, and providing a comprehensive view of potential phishing threats.

**Malware Infections:** Tools like Malwarebytes, Bitdefender, and Kaspersky offer advanced protection against malicious software through detection, removal, and real-time prevention of malware threats.

**DDoS Attacks:** Tools such as Cloudflare, Akamai Kona Site Defender, and Arbor Networks specialize in absorbing increased network traffic and preventing network congestion using advanced DDoS mitigation techniques.

**Ransomware:** Sophos Intercept X, Acronis Cyber Protect, and SentinelOne represent advanced solutions for ransomware protection, offering functionalities such as anomaly detection, data encryption blocking, and rapid incident response.

The suggested tools enable organizations to further strengthen their security posture and effectively address specific threats. Their application, combined with existing security measures, significantly enhances resilience to modern cyber-attacks.

In Fig. 7 we visually represent the number of recommended tools for protection against various types of cyber-attacks. The highest number of tools is recommended for ransomware and DDoS attacks, while specific tools are proposed as additions to basic security measures for phishing and malware infections. This analysis allows organizations to effectively prioritize security solutions based on the threats to which they are most exposed.

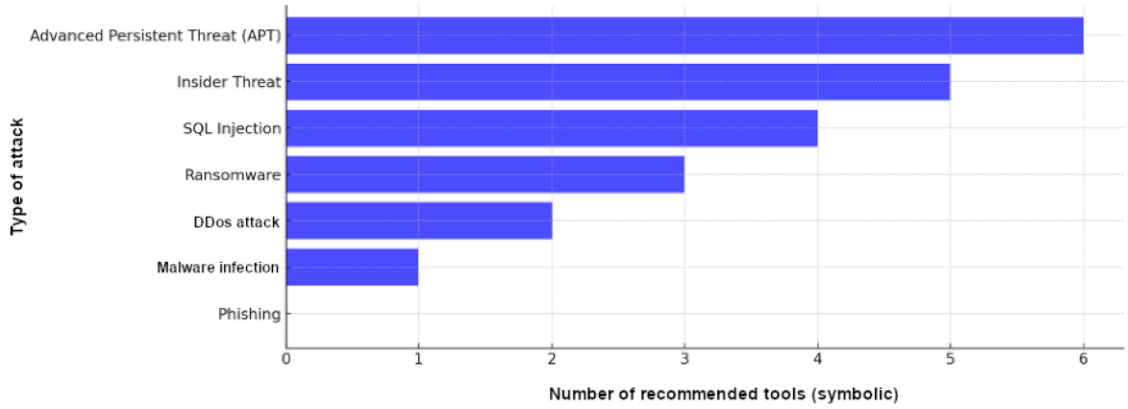


*Fig. 7 Number of tools for cyber-attack prevention*

## 4. STATISTICAL ANALYSIS

### 4.1. Pearson Correlation

In Table 4, we present the Pearson correlation values between various types of protection against cyber-attacks, including phishing, malware, DDoS, and ransomware protection.

*Table 4. Pearson Correlation*

| | **Phishing Protection (score)** | **Malware Protection (score)** | **DDoS Protection (score)** |
|---|---|---|---|
| **Phishing Protection (score)** | 1.0 | -0.3117450666733545 | 0.7420750488816065 |
| **Malware Protection (score)** | -0.3117450666733545 | 1.0 | 0.008868817706475723 |
| **DDoS Protection (score)** | 0.7420750488816065 | 0.008868817706475723 | 1.0 |
| **Ransomware Protection (score)** | 0.7805380298978868 | -0.11177545850247382 | 0.9889370067189437 |

From the table, the following conclusions can be drawn:

- Correlation coefficients indicate the interconnection of the effectiveness of these protective methods. The value of 1.0 on the diagonal shows perfect correlation of each system with itself, which is expected.
- There is a significant positive correlation between Phishing Protection and DDoS Protection (0.742), suggesting that phishing protection measures can also contribute to improved resilience against DDoS attacks.
- Ransomware Protection exhibits the strongest positive correlation with DDoS Protection (0.989), emphasizing the importance of integrated protection systems for more effective management of multiple threats.
- The negative correlation between Phishing Protection and Malware Protection (-0.312) indicates potential differences in the approach or focus of these security solutions, which could result from specific defense needs against these threats.

On the heatmap presented in Fig. 8, we visually depicted these correlations, making it easier to identify positive and negative relationships among different types of protection.

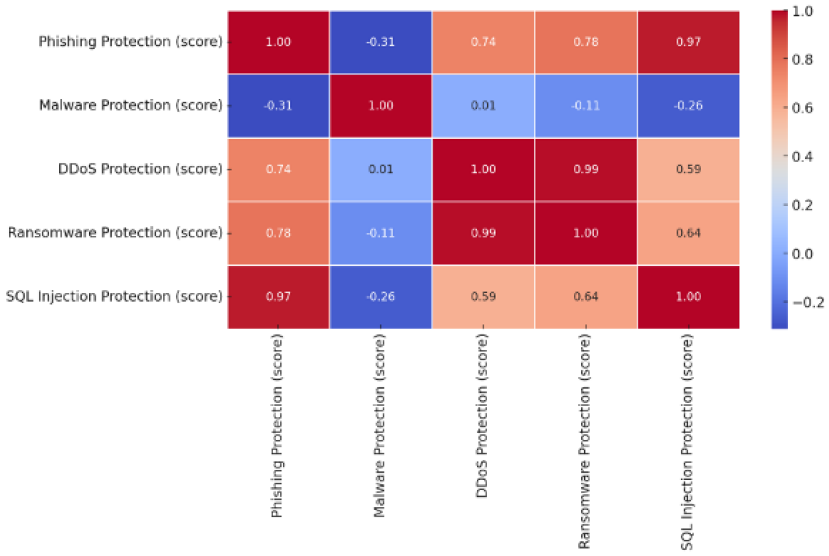


*Fig. 8 Pearson correlation of protective measures*

The strongest correlations are observed between Ransomware Protection and DDoS Protection, while weaker correlations are noted between Malware Protection and other parameters.

## 4.2. Spearman Correlation

In Table 5, we present the Spearman correlation values between various types of protection against cyber-attacks, including phishing, malware, DDoS, and ransomware protection.

Spearman correlation measures the monotonic relationship between variables, enabling an analysis of the hierarchical connection between the efficiency of different protection systems.

*Table 5. Spearman Correlation*

| | **Phishing Protection (score)** | **Malware Protection (score)** | **DDoS Protection (score)** |
|---|---|---|---|
| **Phishing Protection (score)** | 1.0 | -0.3 | 0.8 |
| **Malware Protection (score)** | -0.3 | 1.0 | 0.0 |
| **DDoS Protection (score)** | 0.8 | 0.0 | 1.0 |
| **Ransomware Protection (score)** | 0.8 | 0.0 | 1.0 |

From the table, the following conclusions can be drawn:

- There is a strong positive correlation between Phishing Protection and DDoS Protection (0.8), indicating that improving efficiency in one area may be associated with enhanced protection in the other.

- The correlation coefficient between Malware Protection and other types of protection (0.0) suggests a lack of significant connection, highlighting the need for a specialized approach to implementing malware protection.
- Ransomware Protection also shows strong correlations with both Phishing Protection (0.8) and DDoS Protection (0.8), underscoring the importance of integrated security strategies.

We illustrate Spearman correlation values between individual protection systems on Fig. 9 through various color shades – blue indicates negative correlation, while red represents positive correlation.

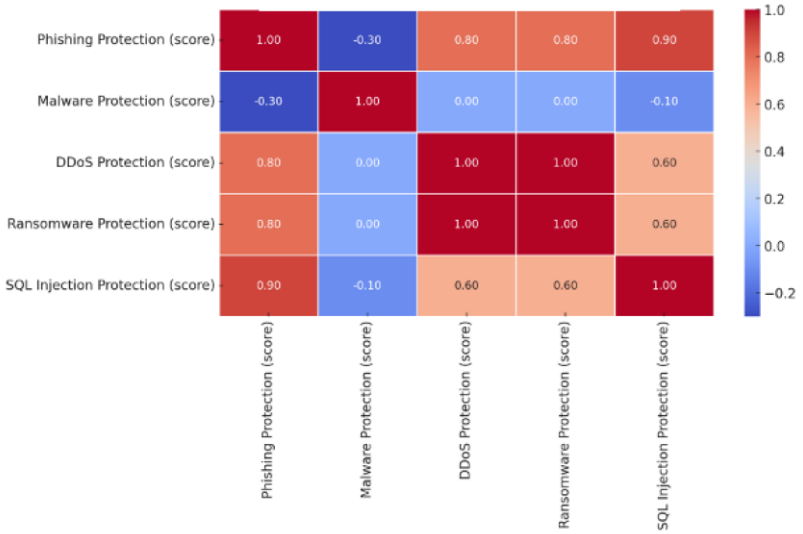


Fig. 9 Spearman correlation of protective measures

Phishing Protection shows a strong positive correlation with DDoS Protection (0.8) and Ransomware Protection (0.8), suggesting the possibility of a synergistic effect among these security systems. Malware Protection has a neutral relationship with other forms of protection (0.0), implying the need for tailored solutions to detect malicious software. SQL Injection Protection demonstrates a strong correlation with Phishing Protection (0.9), highlighting the potential for joint improvements in these areas.

The visual representation allows for quick identification of the strongest relationships, particularly between Ransomware Protection and DDoS Protection, whose correlation (1.0) indicates the potential to optimize resources through integrated solutions.

### 4.3. Kendall Correlation

In Table 6 we present the Kendall correlation coefficients between various forms of protection against cyber-attacks, including phishing, malware, DDoS, and ransomware protection.

Kendall correlation measures the rank-based relationship between variables, allowing an understanding of how closely their rankings align or differ.

*Table 6. Kendall correlation*

| | Phishing Protection (score) | Malware Protection (score) | DDoS Protection (score) |
|---|---|---|---|
| **Phishing Protection** | 1.0 | -0.19999999999999998 | 0.6 |
| **Malware Protection (score)** | -0.19999999999999998 | 1.0 | -0.19999999999999998 |
| **DDoS Protection (score)** | 0.6 | -0.19999999999999998 | 1.0 |
| **Ransomware Protection (score)** | 0.6 | -0.19999999999999998 | 0.9999999999999999 |

From the table, the following conclusions can be drawn:

- A strong positive correlation (0.6) between Phishing Protection and DDoS Protection, as well as between Ransomware Protection and both of these parameters, indicates that phishing and ransomware protection systems often contribute to more effective defense against DDoS attacks.
- A neutral or weak negative correlation (-0.2) between Malware Protection and other parameters suggests that malware protection strategies have little to no overlap with other security solutions
- An exceptionally high positive correlation between Ransomware Protection and DDoS Protection (practically 1.0) underscores a very close relationship in the efficiency of these protection systems

On the heatmap presented in Fig. 10, we visually depict Kendall correlation values between various types of cyber protection systems. Color shades range from blue (negative correlation) to red (positive correlation), with color intensity indicating the strength of the correlation.

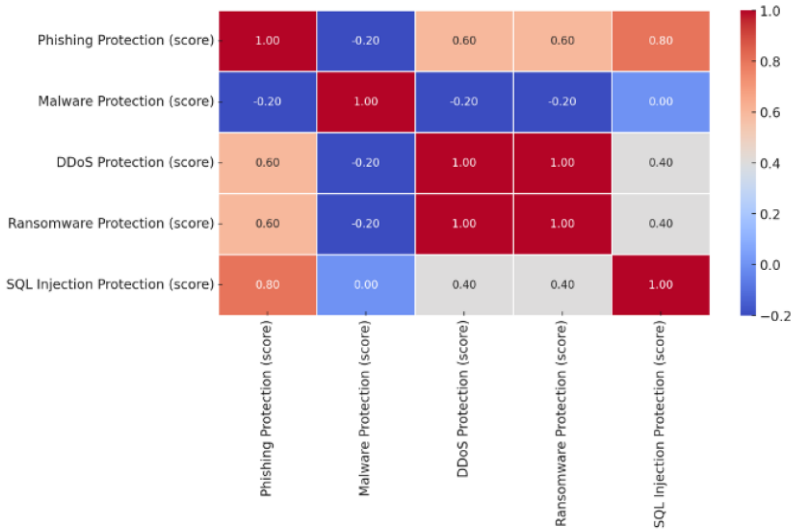


*Fig. 10 Kendall correlation of protective measures*

The visualization enables quick identification of relationships between variables, providing users with intuitive insights into the data and potential strategies for optimizing security systems.

A strong positive correlation between Phishing Protection and DDoS Protection (0.6), as well as between Ransomware Protection and both of these parameters, can be observed. The negative correlation between Malware Protection and other types of protection (-0.2) indicates weaker connections of this system with other security methods.

This analysis emphasizes that while strong connections exist between certain security systems, individual strategies must be further optimized to achieve higher levels of protection against specific threats.

### 4.4. Statistical Methods Used to Analyze Correlations of Cyber-Attack Protection Measures

In this analysis, we used three main correlation methods to examine relationships between different security measures (Anderson, 2020):

1. *Pearson Correlation* (r)

   **Formula:**

$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2}\sqrt{\sum(Y_i - \bar{Y})^2}}$$

   **Explanation:** This method measures the linear relationship between two variables. Values range between -1 and 1, where:

   - Close to 1 – strong positive correlation
   - Close to -1 – strong negative correlation
   - Close to 0 – no significant correlation

2. *Spearman Correlation* (ρ)

   **Formula:**

$$\rho = 1 - \frac{6\sum d_i^2}{n(n^2 - 1)}$$

   **Explanation:** The Spearman coefficient is used to examine monotonic relationships between variables (i.e., not necessarily linear relationships, but if one variable increases, the other consistently increases or decreases).

3. *Kendall Correlation* (τ)

   **Formula:**

$$\tau = \frac{C - D}{C + D}$$

   **Explanation:** This method examines the similarity of order between two variables, focusing on data pairs and their relative rankings.

### 4.5. Input data

We entered protection ratings for five types of cyber-attacks (Tipton & Krause, 2019): Phishing Protection, DDoS Protection, Ransomware Protection and SQL Injection Protection

### 4.6. Results of the analysis

- The strong correlation between protection against phishing and SQL injection indicates that organizations using advanced email filters often also implement protection against malicious data inputs.
- DDoS protection is treated as a separate entity, suggesting that organizations invest in it independently of other security measures.
- Robust ransomware protection often goes hand in hand with phishing protection, showing that these types of attacks are frequently linked in real-world scenarios.

## 5. CONCLUSION

Data security is becoming an increasingly important aspect of corporate operations, especially in the context of rising cyber threats. An analysis conducted on 50 companies in Bosnia and Herzegovina revealed that most companies utilize protective measures, but their effectiveness varies depending on the level of implementation and the security tools used.

The results of the statistical analysis show that companies using paid security tools and implementing comprehensive protective measures have a significantly lower probability of cyber-attacks. A notable finding is the strong correlation between protection against phishing attacks and SQL injections, suggesting that companies investing in email security often have better protection in database security as well.

DDoS attacks have proven to be particularly challenging to prevent, as their mitigation requires advanced network technologies such as CDN services and firewall solutions. On the other hand, phishing attacks are among the easiest to prevent through employee training and the implementation of email filters.

**REFERENCES**

Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Hoboken: Wiley, 2020.

Desolda, Giuseppe, and Rosanna Ferro. Human Factors in Phishing Attacks. Springer, 2022.

Salkić, Haris, Nihad Korajlić, and Mehmed Zajmović. Digitalna forenzika kroz praktične primjere. Sarajevo: IUVKS-Internacionalno udruženje vještaka kriminalističke struke, 2025.

Schneier, Bruce. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. New York: W.W. Norton & Company, 2019.

Stallings, William, and Lawrence Brown. Computer Security: Principles and Practice (4th ed.). New York: Pearson, 2018.

Tipton, H. F., & Krause, M. Information Security Management Handbook (6th ed.). CRC Press, 2019.

Whitman, Michael E., and Herbert J. Mattord. Principles of Information Security (7th ed.). Boston: Cengage Learning, 2022.

Bose, Indranil, and Ada C. M. Leung. "The impact of security breaches on firms' digital transformation initiatives." Journal of Cybersecurity 5, no. 2 (2019): 1–15.

Bhuvana, A., Gaurav Bhat, and Praveen Shetty. "DDoS Attack Mitigation Strategies: An Analysis." Network Security Journal 12 (2021): 45–60.

Jalali, Mohammad S., and Joseph P. Kaiser. "Cybersecurity in healthcare: A systematic review of modern threats and solutions." Computers & Security 94 (2020): 101–113.

Smith, George. "The rise of ransomware attacks: Strategies for prevention and mitigation." Cybersecurity & Privacy Journal 3, no. 1 (2021): 45–58.
Clean Email. "Advanced Threat Filtering for Email Security." Clean Email Security Blog, 2025. https://clean.email
Cloudflare. "DDoS Attack Prevention Solutions." Cloudflare Network Insights, 2024. https://www.cloudflare.com
Datto. "Cybersecurity Solutions for Businesses." Datto Reports, 2024. https://www.datto.com
ENISA. "Threat Landscape Report 2023: Cyber Threat Trends and Insights." European Union Agency for Cybersecurity, 2023. https://www.enisa.europa.eu
Fortinet. "Corporate Security Policies." Fortinet Research, 2025. https://www.fortinet.com
Hornetsecurity. "Securing Backup Systems Against Ransomware." Hornetsecurity Blog, 2023. https://www.hornetsecurity.com
Huawei Cloud. "Comprehensive Load Balancing Solutions." Huawei Insights, 2025. https://www.huaweicloud.com
IP2Location. "Geolocation-Based Security Tools." IP2Location Security Tools, 2024. https://www.ip2location.com
LevelBlue. "Enhanced Access Control Systems for Enterprises." LevelBlue Whitepaper, 2024. https://www.levelblue.com
OWASP. "OWASP Top Ten Security Risks for 2025." Open Web Application Security Project, 2025. https://owasp.org
SentinelOne. "Ransomware Protection with AI-Powered Defense." SentinelOne Reports, 2025. https://www.sentinelone.com
Teramind. "User Activity Monitoring and Insider Threat Detection." Teramind Insights, 2025. https://www.teramind.com
Threatcop. "Phishing Prevention Strategies." Threatcop Blog, 2022. https://www.threatcop.com
Verizon. "Data Breach Investigations Report 2023." Verizon Enterprise, 2023. https://www.verizon.com/business/resources/reports/dbir/
Vumetric. "Validation and Input Filtering Against SQL Injections." Vumetric Blog, 2025. https://www.vumetric.com

***Notes on the authors***

**Hadžib Salkić**, CEPS - Center for Business Studies Kiseljak, Bosnia and Herzegovina
**Nedžad Korajlić**, CEPS - Center for Business Studies Kiseljak, Bosnia and Herzegovina,
**Dušan Rajčević**, Faculty for Applied Management, Economy and Finance, Belgrade, Serbia