International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 13 Issue 1 ǁ January 2025 ǁ PP. 115-121

Evaluating personal information security based on analytic hierarchy process

Lin Yihan
Guanghua Cambridge International School

Abstract: *This paper analyzes the current situation of personal information security risk assessment, explore its influencing factors and coping strategies. Through reviewing the relevant literature and empirical research, we find that although the research on personal information security assessment has made some progress at home and abroad, there are still some problems and challenges. To address these, this paper applies the analytic hierarchy process (AHP) to identify critical security factors, finding that software and system integrity are paramount in ensuring the protection of personal information. The paper concludes by discussing the implications of these findings and suggesting directions for future research.*
Keyword: *Information Security, Risk Assessment, Analytic Hierarchy Process, Criterion*

Date of Submission: 17-01-2025 Date of acceptance: 31-01-2025

I. Introduction

With the rapid growth of the Internet and the dawn of the big data era, information systems and networks have become deeply intertwined with our daily live. At the same time, however, the increasing storage and transfer of personal information online have heightened the risk of data breaches. Frequent cyberattacks, such as hacker intrusions and data leaks, have made personal information security a critical issue, posing potential threats to both businesses and individuals. For example, in the first half of 2024, several large-scale data breaches shocked the world, affecting major companies like telecom giant AT&T and prominent U.S. healthcare IT firms. These incidents exposed over a billion records and reminded us of the vulnerabilities in our systems. According to Crowdstrike's *2024 Global Cybersecurity Threat Report*, the most pressing cybersecurity threats today include identity-based social engineering attacks, cloud technology exploitation, and misuse of third-party relationships.

The Paper reported that Cybersecurity Association of China's 2024 mid-year cybersecurity analysis highlighted a total of 141.71 billion attacks targeting Web systems, marking a 61.39% year-over-year increase, and 3.534 billion IPv6 protocol attacks, up by 87.78%, underscoring the severe cybersecurity landscape [8].

Globally, personal information protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Personal Information Protection Law in China, has promoted the importance of personal information security. Research into personal information security not only aims to prevent unauthorized access and misuse of personal data but also safeguards privacy rights, mitigates social issues stemming from information leaks, maintains societal order, and builds public trust in digital platforms through effective security measures. Additionally, studies in this field drive advancements in emerging technologies, such as encryption and blockchain, to enhance personal information protection.

Based on these factors, this paper aims to make a systematic quantitative assessment of risk factors of personal information security by using AHP. Analytic hierarchy process (AHP) is a multi-criteria decision-making method, which can classify complex problems and effectively help decision makers identify and rank the relative importance of different risk factors. By constructing a hierarchical model of personal information security risk, this paper hopes to provide a more scientific risk assessment method, and provide theoretical basis and practical guidance for the protection of privacy of enterprises and individuals.

II. Information security risk assessment methods and standards

2.1 Overview of assessment methodology

According to the different calculation methods, the current assessment methods can be divided into three categories: qualitative and quantitative information security risk assessment methods and qualitative and quantitative information security risk assessment methods.[18][19]

(1) Qualitative information security risk assessment method is mainly based on the researcher's experience knowledge, policy trend, historical lessons and special cases and other non-quantitative data to judge the risk status of the assessed system. Qualitative analysis mainly depends on the subjective analysis of the evaluator, which requires higher ability of the evaluator, but its evaluation is more comprehensive. Common

qualitative analysis methods include Delphi method, logical analysis method, historical comparison method, etc.

(2) Quantitative analysis is to evaluate risks through quantified indicators, and the objectives of analysis and measures to be taken are relatively more specific, reliable and clear, and relatively considerable. However, quantitative analysis is easy to simplify the original complex problem in the quantitative process, but this method can make the data clearer and more intuitive to be displayed. Common methods include regression model, time series model, cluster analysis, etc.

(3) The risk assessment method combining qualitative and quantitative analysis effectively combines the former two, selecting the essence and discarding the dross. In the face of complex risk analysis problems, quantitative analysis is adopted for structured problems, and qualitative analysis is adopted for unstructured problems, which complement each other.

2.2 Information security risk assessment criteria

Information security risk assessment is to conduct a scientific, systematic and comprehensive analysis of the influencing factors and vulnerabilities faced by information systems from the perspective of risk management, and then assess the hazards caused and propose relevant security measures for them.

Since the 1980s, countries around the world began to formulate their own information security assessment standards. At present, the more popular international information security assessment standards include ISO/IEC 27001, Common Criteria (CC) and NIST SP series.

(1) ISO/IEC 27001 is an international standard [1] published jointly by the International Organization for Standardization (ISO) [2][3] and the International Electrotechnical Commission (IEC) to help organizations establish, implement, maintain and continuously improve information security management systems (ISMS) to effectively protect company information assets. The standard covers all aspects of information security, including security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, system acquisition, development and maintenance, information security incident management, and business continuity management.

(2) Common Criteria (CC) is the most comprehensive information technology product and system security assessment criteria in the world. CC aims to provide a common set of requirements for IT product security functions and safeguards to guide the development, evaluation and procurement process of IT products with security functions. The evaluation results can help consumers determine whether the IT product meets their security requirements.

(3) The NIST SP Series is a special series of publications issued by the National Institute of Standards and Technology (NIST) [6][7] containing numerous guidelines and standards for information security. Covering everything from data encryption to cybersecurity, these publications provide important references and guidance for governments and businesses in information security practices.

III. Research technique

3.1 An Introduction to the Analytic Hierarchy Process

This study uses Analytic Hierarchy Process (AHP) [13][14][15]to systematically assess the risk of personal information security. AHP, a multi-criteria decision-making method given by Saaty T.L, a famous American specialist on operation research, in 1970s, can deal with the complex decision-making process effectively. The basic principle of analytic hierarchy process is to regard the decision problem as a system, and then use the relevant mathematical methods to sort the various factors, and finally through the analysis of the results of the sorting to assist decision-making.

The research method of this paper mainly includes the following steps:

(1) Determine the evaluation index system

(2) Establish the hierarchical structure model

(3) Construct the pairwise comparison judgment matrix

(4) Consistency test

(5) Weight calculation and ranking

3.1.1 determine the evaluation index system

In this study, based on literature review and expert interviews, the main risk factors affecting personal information security were identified, including [10][11][12] as follows:

Data security: data collection, storage, transmission, and content security.

Security of infrastructure: security of information systems, operating systems, Mobile device and hardware facilities.

Management mechanism: industry operation and personnel management system, information management security system, etc.

Technical security: including the effectiveness of security software, encryption technology, and other technical means.
External environment: national policies, laws and regulations, and the quality of humanity

3.1.2 Establishing a hierarchical structure model

When using the analytical hierarchy process to solve a problem, the first thing to do is to organize the problem and establish a hierarchical structure model [17]. These levels could be roughly divided into three categories: the highest level (Goal), the middle level (Criteria), and the lowest level (Alternatives). The top level of the hierarchy model was the focus of the goal, and there was only one element, namely the goal level. The criteria level contained a series of links involved in achieving the predetermined goal, including the criteria and sub-criteria that needed to be considered, so there could be several levels of combination. The program level was the options and measures that could be chosen.

3.1.3 Construction of pairwise comparison judgment matrix

In AHP, pairwise comparisons are made to determine the relative importance of risk factors in the assessment. According to AHP methodology, the judgment matrix is constructed by pairwise comparison of all factors using the 1 - 9 scale method proposed by Saaty. Each factor in the criteria layer may not have the same proportion in the goal measurement, and they have different proportions in the decision maker's mind. Experts in the relevant field score each factor to determine the importance ratio between two factors. A pairwise comparison matrix is then formed to calculate the importance of each factor relative to the others in turn. For example, experts comparing "data security" to "infrastructure security" might record a 3 if data security is considered slightly more important. The judgment matrix obtained by pairwise comparison can reflect the relative weights of risk factors more comprehensively.

Thus, in AHP, Saaty introduced 1 to 9 and its reciprocal as scales to define the judgment matrix $A = (a_{ij})_{n*n}$(Table 1), so that the two elements can be quantitatively described [16]

Table 1 Saaty1-9 scale table and its meaning

Scale	meaning
1	Indicates that two factors are of equal importance when compared
3	Indicates that the former is slightly more important than the latter
5	Indicates the former is distinctively more important than the latter
7	Indicates the former is significantly more important than the latter
9	Indicates the former is extremely more important than the latter
2,4,6,8	Represent the median value of the above neighboring judgments
reciprocal	If the importance ratio of factor I and factor j is aij, the importance of factor j and factor i is aij =1/aij

3.1.4 Consistency test

It is impossible to achieve complete consistency due to the pairwise comparison judgment matrix constructed. Therefore, it is allowed that the paired comparison judgment matrix may be inconsistent to a certain extent, but the comparison judgment matrix must also have a certain consistency, so the consistency is verified by the following steps.

(1) Compute consistency index (CI)

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

Where λ_{max} is the largest eigenvalue of the judgment matrix

(2) Comparison and search of average random consistency index RI, RI table given by Saaty is shown in the following figure.

Table 2 Average random consistency index

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
RI	0	0	0.52	0.89	1.12	1.24	1.36	1.41	1.46	1.49	1.52	1.54	1.56	1.58

(3) Calculate consistency ratio (CR)

$$CR = \frac{CI}{RI}$$

When $CR \leq 0.1$,the consistency of the judgment matrix is considered acceptable, otherwise, the matrix is adjusted.

3.1.5 Weight calculation and sorting

Hierarchical single ranking refers to the process of how much each factor in the lower layer affects a certain factor in the upper layer, which can be calculated by feature vector.

Multiply the weight vector W by the weight ratio matrix A to the right,

$$AW = \lambda_{max} W$$

$\lambda_{max}$is the largest eigenvalue of the judgment matrix, exists and is unique, and the components are all positive components. Finally, the weight vector obtained is normalized.
Further calculation of the single sorting results of each layer can obtain the combination weight of all factors in each layer relative to the target layer in the hierarchical structure model, calculated from top to bottom, this process is called hierarchical total sorting.

IV. Application example analysis

We analyze the significance of various risk factors contributing to personal information disclosure using the Analytic Hierarchy Process (AHP). This section outlines the methodology employed to evaluate these risk factors systematically and presents the results of our analysis. The primary goal is to establish a reliable and structured evaluation framework that supports decision-making and risk mitigation strategies in the domain of personal information security. [8][9]

(1) Establish an evaluation system (see Figure 1)
(2) Establish a hierarchy model (as shown in Figure 1)
(3) Establishment of pairwise judgment matrix

Table 3 Importance of personal risk disclosure factors ($\boldsymbol{\lambda_{max}}$**： 5.4084,** consistency ratio:**0.0912)**

Importance of risk factors for personal information disclosure	data security	infrastructure Security	management mechanism	technology security	externalities	W_i
data security	1	1/3	2	1/3	1/4	0.0836
infrastructure Security	3	1	5	1	2	0.2862
management mechanism	1/2	1/5	1	1/5	1/6	0.0475
technology security	3	1	5	1	5	0.3920
externalities	4	1/2	6	1/5	1	0.1907

Table 4 Data safety ($\boldsymbol{\lambda_{max}}$**:**3.0183, consistency ratio: 0.0176)

data security	password management technique	Network behavior safety awareness	Software and System Security	W_i
password management technique	1	3	1/2	0.3196
Network behavior safety awareness	1/3	1	1/4	0.1220
Software and System Security	2	4	1	0.5584

Table 4 highlights the relative importance of three key factors contributing to data security: password management techniques, network behavior safety awareness, and software and system security. The weights (Wi) were determined using AHP, with software and system security emerging as the most significant factor (Wi: 0.5584), indicating its critical role in preventing vulnerabilities. Password management techniques (Wi: 0.3196) were moderately important, emphasizing the need for robust password practices. In contrast, network behavior safety awareness (Wi: 0.1220) held a lower weight, suggesting that while user awareness is valuable, technical safeguards have a more substantial impact on data security. The consistency ratio (CR: 0.0176) confirms the reliability of the pairwise comparisons.

Table 5 Infrastructure Security ($\boldsymbol{\lambda_{max}}$**:3.0536，** consistency Ratio: 0.0516)

infrastructure Security	password management technique	Network behavior safety awareness	Software and System Security	W_i
password management technique	1	4	1/2	0.3445
Network behavior safety awareness	1/4	1	1/4	0.1085
Software and System Security	2	4	1	0.5469

Table 5 summarizes the relative importance of the factors affecting infrastructure security, with the weights (Wi) calculated through AHP. Software and system security stands out as the most critical factor (Wi: 0.5469), reflecting its pivotal role in ensuring the stability and resilience of infrastructure. Password management techniques (Wi: 0.3445) follow, emphasizing their importance in maintaining secure access to systems. In contrast, network behavior safety awareness (Wi: 0.1085) is assigned a lower weight, indicating its relatively minor influence in this context. The consistency ratio (CR: 0.0516) ensures the validity of the pairwise comparisons and confirms the reliability of the results.

Table 6 management mechanism (λ_{max}:3.0649，consistency Ratio: 0.0624)

management mechanism	password management technique	Network behavior safety awareness	Software and System Security	W_i
password management technique	1	3	1/5	0.1884
Network behavior safety awareness	1/3	1	1/7	0.0810
Software and System Security	5	7	1	0.7306

Table 6 presents the analysis of factors influencing the management mechanism, with weights (Wi) derived using AHP. Software and system security is identified as the most significant factor (Wi: 0.7306), indicating its dominant role in ensuring effective management mechanisms for personal information security. Password management techniques (Wi: 0.1884) are moderately important, highlighting their contribution to maintaining secure administrative access. On the other hand, network behavior safety awareness (Wi: 0.0810) is assigned the lowest weight, suggesting a comparatively limited impact in this category. The consistency ratio (CR: 0.0624) confirms the reliability and logical consistency of the pairwise comparisons.

Table 7 technology security (λ_{max}:3.0026，consistency Ratio: 0.0025)

technology security	password management technique	Network behavior safety awareness	Software and System Security	W_i
password management technique	1	7	1	0.4761
Network behavior safety awareness	1/7	1	1/6	0.0716
Software and System Security	1	6	1	0.4523

Table 7 illustrates the analysis of factors contributing to technology security, with weights (Wi) determined through AHP. Password management techniques are identified as the most significant factor (Wi: 0.4761), emphasizing their critical role in maintaining robust security within technological systems. Software and system security closely follows with a weight of 0.4523, reflecting its essential contribution to safeguarding information. In contrast, network behavior safety awareness (Wi: 0.0716) is assigned the lowest weight, indicating its comparatively minor influence in this domain. The consistency ratio (CR: 0.0025) confirms excellent consistency in the pairwise comparisons, ensuring the reliability of these results.

Table 8 externalities (λ_{max}:3.0055，consistency Ratio: 0.0053)

externalities	password management technique	Network behavior safety awareness	Software and System Security	W_i
password management technique	1	1/5	1	0.1488
Network behavior safety awareness	5	1	4	0.6908
Software and System Security	1	1/4	1	0.1603

Table 8 highlights the analysis of factors influencing externalities, with weights (Wi) derived using AHP. Network behavior safety awareness emerges as the most significant factor (Wi: 0.6908), indicating its critical role in addressing external risks, such as third-party actions and social engineering. Software and system security (Wi: 0.1603) holds moderate importance, reflecting its contribution to mitigating external vulnerabilities. Password management techniques (Wi: 0.1488) are assigned the lowest weight, suggesting a relatively limited impact within this category. The consistency ratio (CR: 0.0053) ensures high reliability and consistency of the pairwise comparisons.

(4) Consistency test

Table 9 Consistency test table

element	weight	CI	RI（ order ）	CR
Alternatives				
Software and System Security	0.4458	\	\	
password management technique	0.3493	\	\	
Network behavior safety awareness	0.2049	\	\	
Criteria				0.0212
technology security	0.3920	0.0013	0.5200（3）	0.0025
infrastructure Security	0.2862	0.0268	0.5200（3）	0.0516
externalities	0.1907	0.0028	0.5200（3）	0.0053
data security	0.0836	0.0091	0.5200（3）	0.0176

management mechanism	0.0475	0.0324	0.5200（3）	0.0624

(5) Weight calculation and sorting

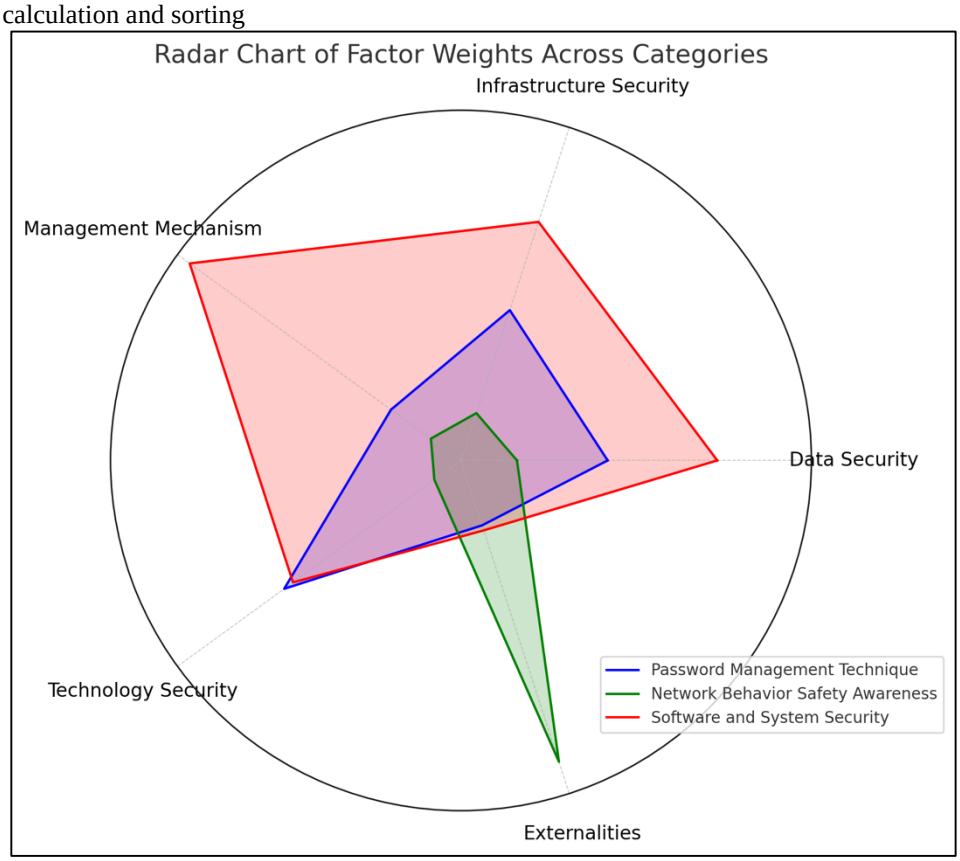

Fig.1 Comparison of Factor Weights Across Dimensions

This radar chart visualizes the relative weights of three key factors—Password Management Technique, Network Behavior Safety Awareness, and Software and System Security—across five primary dimensions: Data Security, Infrastructure Security, Management Mechanism, Technology Security, and Externalities. These weights were derived using the Analytic Hierarchy Process (AHP), which provides a structured evaluation of their importance in mitigating personal information disclosure risks.

From the chart, several key observations emerge.

i) Software and System Security consistently holds the highest importance across most dimensions, particularly in Management Mechanism and Infrastructure Security, underscoring its critical role in ensuring robust and secure systems.

ii) Password Management Technique shows moderate significance, especially in Technology Security and Infrastructure Security, highlighting its contribution to maintaining secure access controls.

iii) Network Behavior Safety Awareness, while less impactful in most dimensions, dominates in Externalities, indicating its relevance in mitigating risks associated with external factors such as social engineering and third-party vulnerabilities.

The radar chart effectively complements the quantitative results presented in Table 10 by offering a clear, visual representation of how the factors' weights are distributed across dimensions. This visualization not only highlights the dominant role of technical safeguards but also provides insights into areas requiring improvement, such as enhancing user awareness under critical dimensions like Data Security.

V. Conclusion

Based on the analytic hierarchy process (AHP) used in this paper, we conclude that the relative risk of software and system security is the largest, and the relative risk of personal network behavior security awareness is the smallest.

With the rapid development of information technology, it undoubtedly brings great impetus to social progress, but the security problems caused using information technology should not be underestimated. Therefore, effective risk assessment of personal information security is of great significance both in theory and in practice.

To sum up, this paper makes deep research on information security risk assessment methods, and puts forward some improvements on the original quantitative methods of risk assessment. However, there are still many aspects that need to be further expanded and deepened.

(1) In AHP, the division of hierarchy can be more detailed and there can be more levels; and due to the complexity of the system, not only the relationship between system risks, but also the inherent relationship between various factors should be considered. Objective data can be transformed into judgment matrix in AHP, which can make evaluation more objective.

(2) Qualitative scale itself also needs reform. In AHP, the scale standard is too single, and it is best to mark it independently by multiple experts for reference.

(3) AHP is a hierarchical weight decision analysis method, which hierarchizes complex problems and indexes components that affect system objectives to quantify factors that affect decision makers 'subjective judgments. Therefore, it is inevitable to lack some objectivity.

The problems raised in this paper and their solutions are not only applicable to multi-level evaluation, but also applicable to general function, value or benefit evaluation.

References

[1] Xie Zongxiao, Wang Jingyi, Evolution of ISO/IEC 27001 and ISO/IEC 27002 Standards, China Standards Review, 2015 (07)
[2] ISO/IEC 15408-1, Information Technology-Security Techniques-Common Criteria for IT Security Evaluation (CCISE)-Part 1: General Model[S]. 1999, 12.
[3] ISO/IEC 15408-2, Information Technology-Security Techniques-Common Criteria for IT Security Evaluation (CCISE)-Part 2: Security Functional Requirements [S].1999, 12.
[4] ISO/IEC 15408-3, Information Technology-Security Techniques-Common Criteria for IT Security Evaluation (CCISE)-Part 3: Security Assurance Requirements[S].1999, 12.
[5] Bouti A, Ait Kadi. D. A State-of-the-art Review of FMEA [J. International Journal of Reliability, Quality and Salty Engineering. 1994. L515-543.
[6] https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
[7] Wang Huili, Liu Xiangang, Li Haidong, US NIST Information Security Standard Exploration of Security Science and Technology, 2018 (01)
[8] Wang Yingluo. Systems engineering [M]. Four pages. Beijing: Machinery Industry Press, 2012:130
[9] GB/T 20984-2007 Information Security Technology-Information Security Risk Assessment Specification [S], National Standard of the People's Republic of China, 2007.
[10] Feng Dengguo, Zhang Yang, Zhang Yuqing. Review of Information Security Risk Assessment [J]. Journal of Communication. 2004, 25 (7). 10 -18.
[11] Jack A. Jones, An Introduction to Factor Analysis of Information Risk (FAIR)[R].2005.
[12] Yacov Y. Haimes. Risk Modeling, Assessment, and Management [R]. Wiley-Interscience.2002.
[13] Satty, T.L. The Analytic Hierarchy Process [M]. New York: McGraw-Hill,1980.
[14] Xu Shubai. Principles of Analytic Hierarchy Process [M1], Tianjin: Tianjin University Press, 1993.
[15] Satty, T.L. How to make a decision: The Analytical Hierarchy Process [J]. European Journal of Operational Research. 1990, 48.9-26.
[16] Satty, T.L. Fundaments of Decision Making and Priority Theory with the Analytic Hierarchy Process [M]. RWS Publication, 1994.
[17] Wang Lianfen, Xu Shubai, An Introduction to Analytic Hierarchy Process [MI], Beijing: Renmin University of China Press, 1990.
[18] Zhang Jin, Research on Personal Information Security Assessment Based on Analytic Hierarchy Process [A], School of Computer Science, Guangdong Normal University of Technology, 2018.05.024
[19] Wu Jiacheng, Yu Xiao, Research Review of Network Security Risk Assessment Methods [A], Nanjing, 2024. 03. 002