Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

Identifying and ranking the factors affecting the leakage of organizational information using the analytical hierarchy process

Abdulamir Mabhoot [1] | **Mohammad Reza Farhadpoor** [2]✉ | **Ebrahim Hoseini** [3]

1. Information Technology Management-Information Resource Management Departement, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran. **E-mail:** mabhoot.a.a@gmail.com
2. Corresponding author, Information and Knowledge Science-Information Management Departement, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran. **Email:** M.farhadpour@iauahvaz.ac.ir
3. MSc., Information Science and Knowledge, Central Library of Urmia University, Urmia, Iran. **E-mail:** e.hoseini@urmia.ac.ir

Article Info

Article type:
Research Article

Article history:
Received 13 January 2024
Received in revised form 14 May 2024
Accepted 17 May 2024
Published online 14 June 2024

Keywords:
Leakage of Organizational Information,
Information Security,
Information Confidentiality,
Information Flow,
Information Policies of the Organization .

ABSTRACT

Today, organizational information leakage is one of the basic challenges of managers and policymakers because it takes away the opportunity to create value from information assets. therefore, The purpose of this study was to identify and rank the factors affecting organizational information leakage in Ahvaz International Airport using the Hierarchical Analysis Process.

This study is applied in terms of purpose and descriptive in terms of method. In this research, the opinions of 15 employees of Ahvaz International Airport were used. The process of the research included two main steps. In the first step, the set of factors affecting organizational information leakage was identified using the Delphi method in order to reach a consensus. In the second step, the data obtained from the questionnaire was analyzed using the hierarchical analysis process and Expert Choice software.

Based on the results, 5 main factors and 21 sub-factors affecting organizational information leakage were identified. The weighting and prioritization of indicators showed that intentional individual factors (0.277) ranked first, unintentional individual factors (0.235) ranked second, organizational factors (0.188) ranked third, infrastructural factors (0.167) ranked fourth and environmental factors (0.133) ranked fifth.

The results showed that information leakage is a complex phenomenon that various individual, organizational, infrastructural and environmental factors are involved in its occurrence. However, the first and second rank of the intentional and unintentional dimensions of information leakage by individuals, on the one hand, indicate the complexity of the information leakage phenomenon, and on the other hand, require a review in the strategies related to human resources management in Ahvaz International Airport.

Cite this article: Mabhoot, A., Farhadpoor, M. R., & Hoseini, E. (2024). Identifying and ranking the factors affecting the leakage of organizational information using the analytical hierarchy process. *Human-Information Interaction*, 11(1), 33-57.

Journal of Human-Information Interaction
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

Extended Abstract

Introduction

One of the most important current debates in organizational information security is information leakage. Information leakage, which refers to the unauthorized sharing of information by one organization with another, is one of the serious problems faced by organizations. Information leakage can cause losses to the company and affect its ability to gain a competitive advantage. Information leakage includes two types of leakage or intentional or unintentional disclosure of data or exclusive content to unauthorized persons. Intentional information leakage includes the intentional disclosure of information by employees to unauthorized persons. Deliberate information leakage is often caused by employee dissatisfaction with the company or a motive for personal gain. The main cause of intentional information leakage is revenge or unethical behavior of employees who are willing to betray their company or disclose sensitive information to competitors. In other words, if employees are not aware of how much information to disclose to outsiders, then unwanted/inadvertent information leakage may occur. These cases damage the reputation of the organization, its income and business. As a result, the pervasiveness of this uncertainty about information security in the work environment puts the organization's information assets at risk. In order to minimize or prevent information leakage, it is important to investigate and identify the factors that lead to this happening.

Regardless of the type of information leakage and the related motives, the impact of these actions in itself can lead to financial losses, disruption of the organization, loss of reputation and long-term impact on the organizational culture. Although the phenomenon of information leakage may happen in any organization; But considering the opportunities and values that every organization loses as a result, its importance can be understood. For this reason, the consequences of information leakage will be different from one organization to another, and accordingly, its degree of importance will also be different. The study and identification of factors affecting the phenomenon of information leakage is interesting from several aspects. First, the airport environment with the presence of various airlines is an example of a highly competitive market where the actions and operations of the airport are exposed to the customers. The second point is that the customers of the airport system are heterogeneous and may be people of different nationalities. Third point, the issue of security in airport systems is a complex and interesting phenomenon that is provided by the participation of different organizations. The fourth point is that the flow of information in the airport system is intense, intra-organizational and trans-organizational/cross-border. The fifth point is that the occurrence of an error in the flow of information in airport systems can have unfortunate human, financial, and other consequences. Considering these points, the present study was conducted at Ahvaz International Airport. Preventing information leakage is one of the most important security issues at Ahvaz International Airport. Because with the loss of data, the reputation of the airport is damaged and it loses its customers, it has to pay a high cost to fix the damages, and this will sometimes lead to the destruction of the organization. According to the mentioned contents, this research seeks to answer the

Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

question, what are the factors affecting organizational information leakage in Ahvaz International Airport? How are they ranked? Hence, the purpose of this study was to identify and rank the factors affecting organizational information leakage in Ahvaz International Airport using the Hierarchical Analysis Process.

Methods

Since the ultimate goal of the current research was to improve the understanding of the problem of information leakage as an important concern for the organization and to find a practical solution to reduce it, it is practical research in terms of the goal. Also, from the point of view of nature, the current research is descriptive-exploratory; Because what follows the data follower approach to "describe" and "interpret" the factors affecting organizational information leakage as it is. The research community was all information security experts in different parts of Ahvaz Airport; that by the snowball method (because it was difficult to identify the experts and the possibility of contacting and accessing them) 15 experts in the information security field of Ahvaz Airport (having relevant work experience of more than 15 years, a master's degree or higher and familiar with security issue and information leakage). In this study, the library method was used to compile the theoretical foundations of the research, the background of the research and the design of the decision tree. Then, the field method was used to distribute the five-point paired comparison questionnaire to collect data. The first questionnaire was taken from the research literature and was distributed among 15 experts using the Delphi technique. Opinions were sought from the expert group of the Delphi study, in the form of sending a structured questionnaire with a 5-point Likert scale, consisting of 22 questions, in two rounds with the participation of 15 people, in such a way that first, the first questionnaire consisting of 22 questions was sent to the members of the Delphi group. After distributing and collecting completed questionnaires and evaluating the results of this Delphi round, 5 main factors and 21 important sub-factors were identified (laws and regulations sub-factor with an average of 2.87±83 and a t value of 0.61 was not recognized as significant and was excluded from the questionnaire for the second round) and after twenty days, from the initial opinion poll, the important factors were re-evaluated in order to conduct the next round of Delphi in the form of a questionnaire with 21 questions related to the important sub-factors, the collected data It showed the confirmation of all subfactors. Finally, the data was analyzed using the hierarchical analysis method and using Expert Choice software.

Resultss and Discussion

Based on the results, 5 main factors and 21 sub-factors affecting organizational information leakage were identified. The weighting and prioritization of indicators showed that intentional individual factors (0.277) ranked first, unintentional individual factors (0.235) ranked second, organizational factors (0.188) ranked third, infrastructural factors (0.167) ranked fourth and environmental factors (0.133) ranked fifth.

Conclusion

The results showed that information leakage is a complex phenomenon that various individual, organizational, infrastructural and environmental factors are involved in its

Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

occurrence. However, the first and second rank of the intentional and unintentional dimensions of information leakage by individuals, on the one hand, indicate the complexity of the information leakage phenomenon, and on the other hand, require a review in the strategies related to human resources management in Ahvaz International Airport.

Based on the results, intentional individual factors with a weight of 0.277 were the first effective factors on information leakage in Ahvaz International Airport. Also, among intentional individual sub-factors, personal greed with a weight of 0.232 was the most important sub-factor and the experience of invasion of privacy with a weight of 0.078 was the least important sub-factor. The findings confirmed that intentional information leakage due to human factors should still be of concern to managers. Since it is not possible to abandon human factors in the organizational life cycle of information, managers should accept this challenge and look for appropriate mechanisms. In other words, despite human factors, organizations face the challenge of intentional or unintentional information leakage. Intentional leakage of information in the organization may have happened due to personal greed against organizational interests, where employees are willing to sell the organization's information to competitors for material reasons and prefer their interests over the interests of the organization. Jealousy of a company employee to colleagues or employees of competing companies, being dissatisfied with the company or feeling a grudge for any reason also causes the intentional leakage of information. Disgruntled employees may also intentionally disclose important information to unauthorized parties. Unintentional individual factors with a weight of 0.235 were the second most effective factors on information leakage in Ahvaz International Airport. Also, among unintentional individual sub-factors, negligence with a weight of 0.283 was the most important sub-factor and the use of contract and temporary employees with a weight of 0.133 was the least important sub-factor. An inadvertent leak occurs when an insider inadvertently discloses business-critical information that is not intended to be shared with third parties. Unintentional individual threat is the potential behavior of an individual who has access to the network, system or data of an organization through an accidental act or action, without malicious intent, and causes damage or significantly increases the likelihood of serious damage in the future to confidentiality, integrity Or the value of the organization's information.

Organizational factors with a weight of 0.188 were the third most effective factors on information leakage in Ahvaz International Airport. Also, among the organizational sub-factors, lack of understanding the value of information with a weight of 0.392 was the most important sub-factor and lack of proper intra-organizational communication with a weight of 0.262 was the least important sub-factor. The first is a lack of understanding of the value of information. Employees evaluate information differently depending on the hierarchical level, the type of information and the type of organizational structure. Employees' perception of the value of information is described by various researchers as an important aspect. This lack of awareness leads to the fact that the value of information is not clear, so the negative consequences of information leakage are not taken seriously by them. The second case is inappropriate organizational structure. Large companies are sensitive to data protection in the long term. Smaller companies do not have such extensive awareness. In general, organizational structure in terms of formality and existing control mechanisms may affect information leakage. The third case is the lack of proper communication within the

Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

organization. To achieve shared understanding, communication is required to convey a set of necessary values and norms that define the rules or context of interaction. Infrastructural factors with a weight of 0.167 were the fourth most effective factor on information leakage in Ahvaz International Airport. Similarly, among the infrastructure sub-factors, the weakness of information systems with a weight of 0.418 was the most important sub-factor and the presence of security holes in the network infrastructure with a weight of 0.258 was the least important sub-factor. The first is the weakness of information systems. Buying an incomplete information system and weak design of information systems may cause serious problems for organizations. Mechanisms that insiders use to perform business tasks based on their usual information systems can also be used to steal information assets. To prevent leakage and theft of information, mechanisms and protective measures against these methods should be used. The second case is improper use of physical means of data storage (hard drives, USB, CD, etc.). These days, most of the information inside the organization is stored electronically, the media of this information are hard drives, C drives. D. and U. S. etc.) are physical tools that are likely to be physically stolen. Preventing leakage with these devices requires implementing physical security measures. The third thing is the presence of security holes in the network infrastructure. The organization's networks are one of the essential parts of the organization's information technology infrastructure. There are several types of communication in the network. Internal-to-external communication includes any communication that is initiated within the boundaries of the organization and whose destination is outside the organization.

Finally, environmental factors with a weight of 0.133 were the fifth most effective factors on information leakage in Ahvaz International Airport. Also, among the environmental sub-factors, the stakeholders' request for information about security incidents with a weight of 0.416 was the most important sub-factor and the requirements of business partners with a weight of 0.259 was the least important sub-factor. One of the input sources that shape the behavior of people in an organization is the organizational environment. Employee decisions are influenced by environmental structure, the availability of environmental information, and the relevant meaning that employees assign to environmental information. The first case is the request of stakeholders to inform about security incidents. In the recent era, the demand for the type of information leakage events for companies is more intense, external and internal stakeholders are constantly concerned about maintaining a good public image of the organization. Overall, public interest in data breach incidents appears to exert pressure on organizations, while organizational responses are dynamic and appear to change over time. If stakeholder expectations are ignored and social influence is allowed to run its course, political and legal pressure will build, often leading to negative corporate outcomes. Stakeholder dissatisfaction arises when corporate actions do not meet societal expectations, and the gap between corporate actions and stakeholder expectations widens as public trust declines. Therefore, the greater the employees' understanding of information protection as a social expectation, the greater the perception of public leakage events as a threat to the company's image.

In general, the results show that information leakage is a major concern for organizations. In this context, the more the organization depends on information assets, the more relevant the concern of information leakage becomes. In such a situation, the taste of the competitors is

Journal of Human-Information Interaction
kharazmi University
Online ISSN: 2423-7418
https://hii.khu.ac.ir/

stimulated more and more to think of the necessary mechanism to deal with it by getting the information of the organization, while being aware of the related organization's plans. Therefore, the identification of factors affecting information leakage in the form of 21 sub-factors in 5 groups provided the necessary insight to the managers of Ahvaz airport to strengthen the vulnerable points by adopting the necessary measures such as building trust, strengthening the sense of cooperation, observing professional ethics. , using motivational measures, raising awareness of the value of information, proper training of employees regarding information security, redesigning information systems, and designing targeted programs regarding information storage, sharing, and transfer.

Keywords: Leakage of Organizational Information, Information Security, Information Confidentiality, Information Flow, Information Policies of the Organization.

نشریه تعامل انسان و اطلاعات
https://hii.khu.ac.ir/
شاپا الکترونیکی: ۲۴۲۳-۷۴۱۸
دانشگاه خوارزمی

شناسایی و رتبه‌بندی عوامل مؤثر بر نشت اطلاعات سازمانی به روش فرایند تحلیل سلسله مراتبی

عبدالامیر مبهوت[۱]، محمدرضا فرهادپور[۲]✉، ابراهیم حسینی[۳]

۱. کارشناسی ارشد، گروه مدیریت فناوری اطلاعات- مدیریت منابع اطلاعاتی، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران.
رایانامه: mabhoot.a.a@gmail.com

۲. نویسنده مسئول، گروه علم اطلاعات و دانش‌شناسی، مدیریت اطلاعات، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران.
رایانامه: M.farhadpour@auahvaz.ac.ir

۳. کارشناس ارشد، علم اطلاعات و دانش شناسی، کتابخانه مرکزی دانشگاه ارومیه. رایانامه: e.hoseini@urmia.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت:
۱۴۰۲/۱۰/۲۳
تاریخ بازنگری:
۱۴۰۳/۰۲/۲۵
تاریخ پذیرش:
۱۴۰۳/۰۲/۲۸
تاریخ انتشار:
۱۴۰۳/۰۳/۲۵

کلیدواژه‌ها:
نشت اطلاعات سازمانی،
امنیت اطلاعات،
محرمانگی اطلاعات،
جریان اطلاعات،
سیاست‌های اطلاعاتی سازمان.

چکیده (B Nazanin 12)

هدف: هدف این پژوهش شناسایی و رتبه‌بندی عوامل مؤثر بر نشت اطلاعات سازمانی به روش فرایند تحلیل سلسله مراتبی در فرودگاه بین‌المللی اهواز بود.

روش‌پژوهش: این مطالعه از نظر هدف، کاربردی و از نظر روش توصیفی-اکتشافی است. در این پژوهش از نظرات ۱۵ نفر از کارکنان خبره فرودگاه بین‌المللی اهواز به عنوان نمونه با بکارگیری روش گلوله برفی استفاده شد. فرایند اجرایی پژوهش شامل دو گام اصلی بود. در گام اول مجموعه عوامل مؤثر بر نشت اطلاعات سازمانی از متون مرتبط استخراج شد؛ سپس طی دو مرحله با اعمال نظرات خبرگان اتفاق حاصل شد. در گام دوم تجزیه و تحلیل داده‌های حاصل از پرسشنامه با استفاده از فرایند تحلیل سلسله مراتبی و نرم‌افزار اکسپرت چویس انجام شد و جداول و نمودارهای مربوطه ترسیم گردید.

یافته‌ها: بر اساس نتایج ۵ عامل اصلی و ۲۱ زیرعامل موثر بر نشت اطلاعات سازمانی شناسایی شدند. وزن‌دهی و اولویت‌بندی شاخص‌ها نشان داد که عوامل فردی عمدی (۰/۲۷۷) در رتبه اول، عوامل فردی غیرعمدی (۰/۲۳۵) در رتبه دوم، عوامل سازمانی (۰/۱۸۸) در رتبه سوم، عوامل زیرساختی (۰/۱۶۷) در رتبه چهارم و عوامل محیطی(۰/۱۳۳) در رتبه پنجم جای گرفتند.

نتیجه‌گیری: نتایج پژوهش نشان داد که نشت اطلاعات پدیده‌ای پیچیده است که عوامل مختلف فردی، سازمانی، زیرساختی و محیطی در رخداد آن دخیل‌اند. با این‌حال، رتبه اول و دوم ابعاد عمدی و غیرعمدی نشت اطلاعات توسط افراد از یک‌سو بیان‌گر پیچیدگی پدیده نشت اطلاعات و از سوی دیگر نیازمند بازبینی در استراتژی‌های مرتبط با مدیریت منابع انسانی در فرودگاه بین‌المللی اهواز است.

استناد: مبهوت، عبدالامیر؛ فرهادپور، محمدرضا؛ حسینی، ابراهیم (۱۴۰۳). شناسایی و رتبه‌بندی عوامل مؤثر بر نشت اطلاعات سازمانی به روش فرایند تحلیل سلسله مراتبی. *تعامل انسان و اطلاعات*، ۱۱(۱)، ۳۳-۵۷.

ناشر: دانشگاه خوارزمی تهران.

مقدمه

یکی از مهم‌ترین بحث‌های جاری در امنیت اطلاعات[۱] سازمانی، نشت اطلاعات[۲] است. نشت اطلاعات که به اشتراک غیرمجاز اطلاعات یک سازمان با سازمان دیگر اشاره دارد، یکی از مشکلات جدی پیش روی سازمان‌هاست. تعداد رویدادهای نشت اطلاعات در سال‌های اخیر افزایش یافته است. به عنوان نمونه، در یک حادثه امنیتی، یک سرباز اسرائیلی مکان و زمان حمله آتی را در به روزرسانی وضعیت فیسبوک خود فاش کرد و باعث شد ارتش اسرائیل کل عملیات را لغو کرده و او را از گردان خود اخراج کند (کیم، کیم و چانگ[۳]، ۲۰۱۵؛ راجرز، بنجامین و گوپالاکریشنان[۴]، ۲۰۱۸). این مساله با افزایش روزافزون رسانه‌های مجازی به نگرانی‌های بیشتر مدیران نیز دامن زده است. از این رو، مدیران در مورد استفاده کارمندان از فیسبوک و توییتر و سایر رسانه‌ها و شبکه‌های اجتماعی و مجازی نگران هستند، زیرا منجر به نشت مالکیت معنوی و اطلاعات محرمانه می‌شود (عبدالملوک، چانگ و احمد[۵]، ۲۰۱۳). چنگ، لیو و یائو[۶] (۲۰۱۷) استدلال می‌کنند که نشت اطلاعات می‌تواند باعث ضرر برای شرکت شده و بر توانایی آن در دستیابی به مزیت رقابتی تأثیر بگذارد. نشت اطلاعات شامل دو نوع نشت یا افشای عمدی یا غیرعمدی داده‌ها و یا مطالب انحصاری به اشخاص غیرمجاز است (وونگ، تان، چوآه، تسنگ، وونگ و احمد[۷]، ۲۰۲۱). نشت عمدی اطلاعات شامل افشای عمدی اطلاعات توسط کارکنان به اشخاص غیرمجاز است. از نظر تران، چایلدرهوس و دیکینز[۸] (۲۰۱۶) نشت عمدی اغلب ناشی از نارضایتی کارکنان از شرکت یا انگیزه‌ای برای منافع شخصی است. علت اصلی نشت عمدی، انتقام و یا رفتار غیراخلاقی کارکنانی است که مایل به خیانت به شرکت خود یا افشای اطلاعات حساس به رقبا هستند (آناند و گویال[۹]، ۲۰۰۹؛ تران، و همکاران، ۲۰۱۶). این موارد به اعتبار سازمان و درآمد کسب و کار آن آسیب وارد می‌کنند. از سوی دیگر، اگر کارکنان در مورد اینکه مقدار اطلاعاتی که باید برای افراد خارجی افشا شود، آگاه نباشند، آنگاه نشت اطلاعات ناخواسته/غیرعمد ممکن است اتفاق بیفتد (تران و همکاران، ۲۰۱۶). نتیجه این‌که، فراگیر شدن این عدم اطمینان خاطر از امنیت اطلاعات در محیط کار، دارایی‌های اطلاعاتی سازمان را در معرض خطر قرار می‌دهد (وونگ، تان، گووییندان و کومار[۱۰]، ۲۰۲۱).

برای به حداقل رساندن یا جلوگیری از نشت اطلاعات، مهم است که عواملی را که منجر به وقوع این اتفاق می‌شوند، مورد بررسی و شناسایی قرار گیرند (بلادگود و چن[۱۱]، ۲۰۲۱). پژوهش‌ها به عوامل مختلفی دست یافته‌اند. از نظر عبدالملوک، احمد و چانگ (۲۰۱۰) تئوری رفتار برنامه‌ریزی شده[۱۲] مناسب‌ترین مدل نظری در توضیح عوامل زمینه‌ای است که باعث نشت اطلاعات از طریق شبکه‌های اجتماعی آنلاین می‌شود. هاداش، مولر و مائدچه[۱۳] (۲۰۱۲) به مطالعه دو دسته عوامل محیطی و سازمانی پیش‌بین برای نشت اطلاعات پرداختند. وونگ، تان، تان و تسنگ[۱۴] (۲۰۲۰) نیز عوامل انسانی مؤثر در نشت اطلاعات را مورد مطالعه قرار دادند. ون‌درکلایج، وین و هوف[۱۵] (۲۰۲۰) از مدل توانایی، فرصت، انگیزه- رفتار برای پیشگیری از نشت داده‌ها در سازمان‌های مالی بهره گرفتند.

1. Information security
2. Information Leakage
3. Kim, Kim & Chung
4. Rogers, Benjamin, & Gopalakrishnan
5. Abdul Molok, Chang & Ahmad
6. Cheng, Liu & Yao
7. Wong, Tan, Chuah, Tseng, Wong & Ahmad
8. Tran, Childerhouse & Deakins
9. Anand & Goyal
10. Wong, Tan, Govindan & Kumar
11. Bloodgood & Chen
12. Decomposed Theory of Planned Behaviour
13. Hadasch, Mueller & Maedche
14. Wong, Tan, Tan & Tseng
15. Van der Kleij, Wijn & Hof

صرف نظر از نوع نشت اطلاعات و انگیزه‌های مربوطه، تأثیر این اقدامات به‌خودی خود می‌تواند منجر به زیان مالی، اختلال در سازمان، از دست دادن شهرت و تأثیر طولانی مدت بر فرهنگ سازمانی شود (وانگ و همکاران[۱]، ۲۰۱۹). از این‌رو، شناسایی و رتبه‌بندی عوامل مؤثر بر نشت اطلاعات سازمانی یک مسأله تصمیم‌گیری چندمعیاره است که معیارهای کیفی و کمی را در برمی‌گیرد. روش‌های متفاوتی تاکنون برای حل یک مسأله تصمیم‌گیری ارائه شده است، در این میان روش‌های دلفی[۲] و فرایند تحلیل سلسله مراتبی[۳]، روش مناسبی است؛ زیرا زمانی‌که هم معیارها کمی و هم کیفی باشند قابل استفاده است.

هرچند پدیده نشت اطلاعات ممکن است در هر سازمانی اتفاق بیافتد؛ اما با درنظر گرفتن فرصت‌ها و ارزش‌هایی که هر سازمان در نتیجه آن از دست می‌دهد، می‌توان اهمیت آن را درک کرد. برای همین پیامدهای نشت اطلاعات از یک سازمان به سازمان دیگر متفاوت و بر همین اساس درجه اهمیت آن نیز متفاوت خواهد بود. مطالعه و شناسایی عوامل موثر بر پدیده نشت اطلاعات از چند جنبه حائز توجه است. نخست این که، محیط فرودگاهی با حضور شرکت‌های هواپیمایی مختلف مصداق یک بازار پررقابت است که در آن اقدامات و عملیات فرودگاهی در معرض دید مشتریان قرار دارد. نکته دوم این که، مشتریان سیستم فرودگاهی نامتجانس و ممکن است افرادی از ملیت‌های مختلف باشند. نکته سوم، مساله امنیت در سیستم-های فرودگاهی پدیده‌ای پیچیده و حائز توجه بوده که با مشارکت سازمان‌های مختلف تامین می‌شود. نکته چهارم، جریان اطلاعات در سیستم فرودگاهی شدید، درون سازمانی و فراسازمانی/فرامرزی است. نکته پنجم این که، رخداد خطا در جریان اطلاعات در سیستم‌های فرودگاهی می‌تواند پیامدهای ناگوار انسانی، مالی و غیره داشته باشد. جاشاری[۴] (۲۰۱۵) ترافیک هوایی را به عنوان یکی چالش‌های سیستم فرودگاهی، یک فعالیت پویا تعریف می‌کند که روند آن تا حدی به اقتصاد عمومی جامعه بستگی دارد و تاثیر فناوری اطلاعات، تمرکز بر مسافران، افزایش رقابت، نیاز به فرآیندهای تجاری انعطاف‌پذیرتر، پاسخ سریع‌تر به درخواست‌های مسافران، تمایز خدمات به دلیل رقابت، تصمیم‌گیری سریع‌تر تجاری در تمام سطوح مدیریتی را در زمره عواملی می‌داند که سیاست‌گذاران این حوزه را بر آن داشته است تا برای پاسخ‌گویی به این تغییرات و چالش‌ها، دست به اتخاذ مدل‌های سازمانی جدیدی بزنند و سیستم‌های اطلاعاتی را برای مدیریت جریان اطلاعات و تقویت این پیوند بین بخش‌ها بکارگیرند. ضمن این که، نتایج مطالعات نشان داده است که فقدان اطلاعات تاثیر معناداری بر درک خدمات مسافری در سیستم‌های فرودگاهی دارد (مارتل و سنیواراتنه[۵]، ۱۹۹۰؛ شولز، شولز و فریک[۶]، ۲۰۰۷). اطلاعات موجود در نظام‌های اطلاعاتی فرودگاهی، درک مدیران فرودگاه را تسهیل و به آنها کمک می‌کند تا در پروژه‌های فناوری اطلاعات به طور مؤثر با یکدیگر همکاری کنند، تا عملکرد و قابلیت اطمینان سیستم‌های فناوری اطلاعات بهبود یابد و شاهد افزایش سود و تأخیرهای کمتر در حین اجرای سیستم باشند (پورنل[۷]، ۲۰۱۲). نکته قابل تامل دیگر در خصوص پیامدهای ناگوار نشت اطلاعات عدم دقت اطلاعات و تحریف در اشتراک گذاری اطلاعات است (وانگ و همکاران[۸]، ۲۰۱۹).

با درنظر گرفتن این نکات، مطاله حاضر در فرودگاه بین‌المللی اهواز انجام شد. فرودگاه اهواز در فضایی به وسعت ۱۴۵۰۰ متر مربع شامل ۸۰۰۰ مترمربع فضای ترمینال پروازهای داخلی و ۶۵۰۰ متر مربع فضای ترمینال پروازهای خارجی بنا شده است. شرکت‌های هواپیمایی فعال در این فرودگاه عبارتند از: ایران ایر، آسمان، ماهان، کاسپین، ایرتور، آتا، کارون، سپهران، وارش، کیش ایر، اترک، قشم ایر، تابان و زاگرس. در حال حاضر از اهواز به مقاصد تهران، اصفهان، یزد، رشت، مشهد، کیش، عسلویه، خارک، شیراز، سیری، ساری، گرگان، استانبول، کویت پرواز صورت می‌پذیرد. جلوگیری از نشت اطلاعات، جزء مهم‌ترین مسائل امنیتی در فرودگاه بین‌المللی اهواز است. زیرا با از دست رفتن داده‌ها، اعتبار فرودگاه دچار خدشه شده و مشتریان خود را از دست می‌دهد، هزینه بالایی را در جهت برطرف کردن خسارت‌ها باید بپردازد و این امر گاه منجر به

[1] Wong et al
[2]. Delphi
[3]. Analytic Hierarchy Process (AHP)
[4] Jašari
[5] Martel & Seneviratne
[6] Schultz, Schultz & Fricke
[7] Purnell
[8] Wong et al.

نابودی سازمان خواهد گردید. با توجه به مطالب گفته شده این پژوهش به دنبال پاسخگویی به این سؤال است که عوامل مؤثر بر نشت اطلاعات سازمانی در فرودگاه بین‌المللی اهواز کدامند؟ رتبه‌بندی آنها به چه صورت است؟

پیشینه پژوهش

امروزه اطلاعات برای سازمان‌ها به عنوان یک دارایی ارزشمند و منبعی ارزش آفرین قلمداد می‌شود. این مساله سبب شده است که مانند هر منبع راهبردی و رقابتی دیگر در کانون توجه رقبا قرار گیرد. برای همین سازمان‌ها به دنبال توسعه راهبردهای برای نگهداری، حفاظت و تامین امنیت این دارایی ارزشمند هستند. برای همین در طی دهه‌های این مهم در کانون توجه پژوهش‌گران مختلف نیز واقع شده است. از جمله این مطالعات، پژوهش حسن‌نیا و دهقانی (۱۳۹۲) با عنوان «بررسی روش‌های نشت اطلاعات و راهکارهای جلوگیری از آن» است. نتایج مطالعه نشان داد که روش‌های مختلفی مانند تصادفی و یا با قصد خرابکاری برای نشت اطلاعات وجود دارد؛ لذا جهت کاهش خطرات نشت اطلاعات ضروری است اطلاعات حساس شناسایی و به نحوی مناسب سازماندهی گردد و با ابزارهای امنیتی مناسب محافظت گردد. در مطالعه دیگری، نتایج طالش و فراهی (۱۳۹۵) با عنوان «بررسی روش‌های پیشگیری از نشت اطلاعات» به ارائه الگوریتم‌هایی جهت پیشگیری از نشت اطلاعات منجر شد. نتایج اسمعیلی و کفشیان اهر (۱۳۹۸) با عنوان «به اشتراک‌گذاری اطلاعات، نشت اطلاعات و تحریف اطلاعات در یک زنجیره تأمین غیرمتمرکز با یک تولیدکننده و دو خرده‌فروش رقیب» نتایج نشان داد، اگرچه نشت اطلاعات توسط تولیدکننده منافع او را افزایش می‌دهد، اما خرده‌فروش آگاه‌تر را نیز به اشتراک اطلاعات نادرست که به ضرر تولیدکننده است، ترغیب می‌کند. لشگری و احمدی آبکناری (۱۳۹۸) نیز پژوهشی با عنوان «توسعه و دسته‌بندی قوانین حفظ حریم خصوصی کاربران در شبکه‌های اجتماعی بر حسب نوع نشت اطلاعات» انجام دادند. نتایج نشان داد که مجموعه ویژگی‌های شخصی، مجموعه روابط اجتماعی و مجموعه فعالیت‌های اجتماعی را به عنوان عوامل تهدید کننده دسته‌بندی شد. صادقی، رزاقی و احمدی (۱۴۰۲) مطالعه‌ای با عنوان تعیین مقوله‌های موثر بر نقض حریم خصوصی کاربران در شبکه اجتماعی اینستاگرام را با استفاده از روش پیمایشی و اخذ نظرات کارشناسان (خبرگان) با بهره‌برداری از ابزار پرسشنامه و فن دلفی فازی پرداختند. نتایج نشان داد که مقوله های ده‌گانه شامل تهدیدات بالقوه، مواجهه گروه‌های جنسی و سنی در فضای اینستاگرام، قوانین وضع شده در ایران، ناقضان حریم خصوصی و عناصر تحریک کننده حریم خصوصی، مرز ایمنی کاربران، روش‌های نقض حریم خصوصی و سلامت جسمی و روحی کاربران، آموزش و انگیزش از عوامل موثر بر نقض حریم خصوصی کاربران در فضای اینستاگرام محسوب می شوند. نگهدار، پورقهرمانی و بیگی (۱۴۰۲) نیز به بررسی سیاستگذاری جنایی در نقض امنیت سایبری و رهیافت‌های پیشگیری اجتماعی را با روش توصیفی- تحلیل اسناد در قوانین و اسناد بالادستی ایران پرداختند. نتایج نشان داد که هرچند ایران در تقویت بنیان‌های امنیتی مقابلات سایبری راهبردهای مختلفی اتخاذ کرده است؛ لیکن به چهت نبود سیاستگذاری افتراقی مناسب تاکنون موفق به اتخاذ سازوکارهای پیشگیرانه اجتماعی متمرکز و کارآمد نشده است.

در حیطه موضوع نشت اطلاعات مرور پیشینه‌های خارجی نیز حائز اهمیت است. به عنوان نمونه، نتایج مطالعه عبدالملوک و همکاران (۲۰۱۰) با عنوان «شناخت عوامل نشت اطلاعات از طریق شبکه‌های اجتماعی آنلاین برای حفاظت از اطلاعات سازمانی» نشان داد که تئوری تجزیه یافته رفتار برنامه‌ریزی شده[1] مناسب‌ترین مدل نظری در توضیح عوامل زمینه‌ای است که باعث نشت اطلاعات از طریق شبکه‌های اجتماعی آنلاین می‌شود. در مطالعه دیگری، هاداش و همکاران (۲۰۱۲) پژوهشی با عنوان «بررسی عوامل محیطی و سازمانی پیش‌بین برای نشت اطلاعات ناشی از کاربر: یک مطالعه کیفی» انجام دادند. داده‌های مصاحبه افراد خارجی و افراد داخلی شرکت برای شناسایی عوامل زمینه‌ای و توضیح ارتباط بین آنها تجزیه و تحلیل شدند. گزاره‌های بیان شده به درک اینکه چرا افراد در یک سازمان به خوبی از تهدیدات و سیاست‌های امنیتی سیستم اطلاعات آگاه هستند، کمک می‌کند، در حالی که افراد سازمان دیگر سطح آگاهی امنیت سیستم اطلاعات پایین‌تری دارند. وونگ و همکاران (۲۰۲۰) نیز پژوهشی با عنوان «عوامل انسانی در نشت اطلاعات: استراتژی‌های کاهشی برای یکپارچگی در

[1]. Decomposed Theory of Planned Behavior

اشتراک اطلاعات» انجام دادند. یافته‌ها نشان داد که نشت اطلاعات را می‌توان با مکانیزم حاکمیت انسانی مانند جو اخلاقی سازمانی و فرهنگ امنیت اطلاعات مورد بررسی قرار داد. علاوه بر این، فراوانی بیشتر نشت اطلاعات بر یکپارچگی در اشتراک اطلاعات تأثیر منفی می‌گذارد. ون‌درکلایج و همکاران (۲۰۲۰) نیز پژوهشی با عنوان «کاربرد و آزمون تجربی مدل توانایی، فرصت، انگیزه-رفتار برای پیشگیری از نشت داده‌ها در سازمان‌های مالی» انجام دادند. نتایج نشان داد که توانایی (یعنی دانش) به طور منحصر به فردی با رفتار پیشگیری از نشت داده‌ها مرتبط است و انگیزه و فرصت به طور منحصر به فرد با توانایی مرتبط هستند. هم‌چنین، یافته‌ها نشان داد که اگرچه دانش برای دستیابی به رفتار مطلوب بسیار مهم است، افزایش انگیزه و فرصت ممکن است کلیدی برای تأثیرگذاری بر کسب دانش و در نتیجه رفتار پیشگیری از نشت داده‌ها باشند. در مطالعه دیگری، کاپلوزا، مورائس، پرز و سیموئز[1] (۲۰۲۲) پژوهشی با عنوان «عوامل پیشین نقض قوانین امنیت اطلاعات» را با استفاده از تکنیک‌های مدل‌سازی معادلات ساختاری و هوش مصنوعی با شبکه‌های عصبی، بر اساس اطلاعات جمع‌آوری‌شده از ۳۱۸ کارمند سیستم‌های اطلاعات سازمانی انجام دادند. در این پژوهش یک مدل پیش‌بینی معقول در مورد قصد نقض سیاست‌های امنیت اطلاعات شامل متغیرهای نظیر مجازات درک شده[2]، تمایل به ترک خدمت، گسست اخلاقی[3] و تهاجم به حریم خصوصی[4] ارائه شد. نتایج نشان داد که روابط گسست اخلاقی و مجازات درک شده به طور معناداری بر چنین قصدی تأثیر می‌گذارد.

نتایج مطالعه مدنیک[5] (۲۰۲۳) با عنوان تهدید دائمی برای داده‌های شخصی: عوامل کلیدی ورای افزایش سال ۲۰۲۳ نشان داد که نقض داده‌ها در ۹ ماه ابتدای سال ۲۰۲۳ در مقایسه با سال ۲۰۲۲ حدود ۲۰ درصد افزایش داشته است. به اعتقاد وی این حملات به طور فزاینده‌ای تأثیرگذار هستند؛ زیرا مردم اکنون بیشتر زندگی خود را به صورت آنلاین در معرض دید همگان می‌گذرانند، به این معنی که شرکت‌ها، دولت‌ها و سایر انواع سازمان‌ها اطلاعات شخصی بیشتری را جمع‌آوری می‌کنند. از آنجایی که بیشترین اطلاعات شخصی افراد می‌تواند مورد سوء استفاده قرار گیرد و برای سود قابل توجهی فروخته شود، نقض اطلاعات به یک هدف رو به رشد برای مجرمان سایبری تبدیل شده است. این طبق یافته‌های این مطالعه دو عامل کلیدی شامل حملات باج‌افزارها و تهدید فروشندگان داده‌ها در افزایش تهدید برای داده‌های شخصی نقش داشته‌اند.

دولزل و همکاران[6] (۲۰۲۳) در یک مطالعه با رویکرد کمی به تأثیر عوامل داخلی و خارجی بر نقض داده های بیمارستانی پرداختند. مطالعه با روش پیمایشی و از ۱۰۳۲ بیمارستان در سطح شهرستان‌های اسپانیا جمع‌آوری شد. نتایج نشان داد که حجم کاری بستری بیمار، وضعیت مرکز پزشکی، وضعیت مرکز ترومای اطفال، حساب‌های دریافتی و تعداد ویزیت‌های سرپایی به ترتیب در اولویت اول تا پنجم بودند. ضمن این که، نتایج نشان داد که بین حجم کاری بستری بیمار، نوع تسهیلات و پیامدهای مالی و احتمال نقض داده‌ها رابطه وجود دارد. لی، ژیائو و ژانگ[7] (۲۰۲۳) پژوهشی با عنوان بحران امنیت داده‌ها در دانشگاه‌ها: شناسایی عوامل کلیدی موثر بر حوادث نقض داده‌ها با روش تجربی بر روی نمونه‌هایی از چین انجام دادند. به اعتقاد آنها، محیط‌های دیجیتالی بسیار پیچیده و پویا، دانشگاه‌ها را در برابر خطر نقض داده‌ها بسیار آسیب‌پذیر کرده است. نتایج تحلیل فرضیه‌ها نشان داد افزایش افشای عمومی باعث آسیب‌پذیری در برای تشدید فراوانی نقض داده‌ها می‌شود. هم‌چنین، نتایج نشان داد که، جریان داده‌های فرامرزی میزان نقض داده‌ها را کاهش داده است. علاوه بر این، آنها دریافتند مکانیسمی که توسط آن توان تحصیلی بر نقض داده‌ها تأثیر می‌گذارد، از طریق دو واسطه جریان داده‌های مرزی و افشای آسیب‌پذیری قابل بررسی است. ضمن این‌که، استفاده از پردازش ابری باعث کاهش نقض اطلاعات شد و مشخص شد که

[1]. Cappellozza, Moraes, Perez & Simões
[2]. Perceived penalty
[3]. moral disengagement
[4]. Privacy invasion
[5] Madnick
[6]. Dolezel, Beauvais, Stigler Granados, Fulton & Kruse
[7]. Li, Xiao & Zhang

پردازش ابری عمومی نسبتاً امن‌تر هستند. پذیرش پردازش ابری هم‌چنین به عنوان تعدیل‌کننده بین تأثیر منفی آسیب-پذیری‌ها و تأثیر مثبت جریان داده‌های فرامرزی بر نقض داده‌ها عمل می‌کند. راشر و همکاران[1] (۲۰۲۴) مطالعه‌ای با عنوان ایدل‌لیک[2]: بهره‌برداری از اثرات جانبی حالت بیکاری برای نشت اطلاعات را با روش تجربی –آزمایشگاهی انجام دادند. نتایج نشان داد حملات مبتنی بر اثرانگشت از طریق وب سایت و ویدئویی، همه با امتیاز بالا و سطح خطای استاندارد پایین بدست آوردند؛ که به واسطه آنها، اطلاعات حساس در معرض خطر قرار می‌گیرند. نتیجه این که، هرچند اقدامات مبتنی بر کاهش حملات با توجه به نحوه اجرای وقفه‌ها ممکن است گران باشد، اما نیل به کارآمدی و اثربخشی بیشتر نیازمند مطالعات بیشتر است. بوکه و همکاران[3] (۲۰۲۴) در مطالعه خود با عنوان غلبه بر چالش های کمبود، نشت و ابعاد داده در سیستم های تشخیص نفوذ با مرور نظام‌مند پرداختند. آنها با تاکید بر این‌که، اینترنت اشیا و رایانش ابری به‌عنوان فناوری‌های غیرمتمرکز مبتنی بر اینترنت به سرعت در حال گسترش هستند، منجر به افزایش اطلاعات در تمامی حوزه‌های فنی و تجاری شده اند. از این‌رو، اطمینان از امنیت سیستم‌های اینترنت اشیا به دلیل پیچیدگی‌های موجود در محیط‌های پیوسته و اشتراکی، موضوعی مهم و مبرم است. نتایج مطالعه نشان داد که، هرچند شبکه‌ها توسط سیستم‌های تشخیص نفوذ در برابر تهدیدات سایبری مختلف مانند بدافزارها، ویروس ها و دسترسی‌های غیرمجاز با بکارگیری تکنیک های یادگیری ماشینی و یادگیری عمیق محافظت می شوند؛ با این حال، استفاده مؤثر از این فناوری‌ها به در دسترس بودن، کیفیت و ویژگی‌های داده‌های مورد استفاده وابسته است. نتایج مرور پیشینه نشان داد که عوامل موثر مختلفی در نشت اطلاعات مورد توجه تحقیقات پیشین بوده است (جدول ۱).

جدول (۱). استخراج عوامل مؤثر بر نشت اطلاعات سازمانی

عامل	زیرعامل	منبع
عوامل فردی عمدی	طمع شخصی	وونگ، تان، تان و تسنگ (۲۰۲۰)
	نارضایتی شغلی	وونگ، تان، تان و تسنگ (۲۰۲۰) و مغول (۲۰۲۱)
	گسست اخلاقی	کاپلوزا، مورائس، پرز و سیموئز (۲۰۲۲)
	تجربه تهاجم به حریم خصوصی	کاپلوزا، مورائس، پرز و سیموئز (۲۰۲۲)
	حسادت کارکنان	وونگ، تان، تان و تسنگ (۲۰۲۰)
	عدم اعتماد کارکنان	مغول (۲۰۲۱)
	عدم انگیزه کارکنان	مغول (۲۰۲۱)
عوامل فردی غیرعمدی	سهل انگاری	وونگ، تان، تان و تسنگ (۲۰۲۰)،
	عدم پشتیبانی مدیریت ارشد	هاداش، مولر و مائدچه (۲۰۱۲)
	عدم آموزش مناسب کارکنان	وونگ، تان، تان و تسنگ (۲۰۲۰)،
	نامشخص بودن حوزه وظایف کارکنان جدید	وونگ، تان، تان و تسنگ (۲۰۲۰)،
	استفاده از کارکنان قراردادی و موقتی	تان (۲۰۱۶)
عوامل محیطی	درخواست ذینفعان در جهت اطلاع‌رسانی در خصوص حوادث امنیتی	هاداش، مولر و مائدچه (۲۰۱۲)
	الزامات نظارتی	هاداش، مولر و مائدچه (۲۰۱۲)
	الزامات شرکای تجاری	هاداش، مولر و مائدچه (۲۰۱۲)
	قوانین و مقررات	هاداش، مولر و مائدچه (۲۰۱۲)
عوامل زیرساختی	ضعف سیستم‌های اطلاعاتی	حسن‌نیا و دهقانی (۱۳۹۲)
	استفاده نامناسب از ابزارهای فیزیکی (درایوهای سخت، یو. اس. بی، سی. دی و ...)	حسن‌نیا و دهقانی (۱۳۹۲)
	وجود حفره‌های امنیتی در زیرساخت شبکه	حسن‌نیا و دهقانی (۱۳۹۲)
سازمانی	ساختار سازمانی نامناسب	هاداش، مولر و مائدچه (۲۰۱۲)
	عدم درک ارزش اطلاعات	هاداش، مولر و مائدچه (۲۰۱۲)
	عدم ارتباطات درون سازمان مناسب	هاداش، مولر و مائدچه (۲۰۱۲)

[1]. Rauscher, Kogler, Juffinger & Gruss
[2]. IdleLeak
[3]. Bouke, Abdullah, Udzir & Samian

روش‌شناسی پژوهش

از آن‌جا که، هدف غایی پژوهش حاضر، بهبود درک نسبت به مسئله نشت اطلاعات به عنوان یک دغدغه مهم فراروی سازمان و یافتن راه حل عملی برای کاهش بود، از نظر هدف، پژوهشی کاربردی است. هم‌چنین، از منظر ماهیت، پژوهش حاضر از نوع توصیفی- اکتشافی است؛ چرا که آن‌چه را که رویکرد داده پیرو را دنبال می‌کند تاعوامل موثر بر نشت اطلاعات سازمانی را همان‌گونه که هست «توصیف» و «تفسیر» کند. جامعه پژوهش کلیه کارشناسان حوزه امنیت اطلاعات در بخش‌های مختلف فرودگاه اهواز بودند؛ که با روش گلوله برفی (به جهت این‌که شناسایی خبرگان و امکان تماس و دسترسی به آنها دشوار بود) تعداد ۱۵ نفر از خبرگان حوزه امنیت اطلاعات فرودگاه اهواز (دارای سابقه کار مرتبط بیش از ۱۵ سال، مدرک تحصیلی فوق لیسانس و بالاتر و آشنا به موضوع امنیت و نشت اطلاعات) تشکیل دادند. در این مطالعه از روش کتابخانه‌ای برای تدوین مبانی نظری پژوهش، پیشینه پژوهش و طراحی درخت تصمیم‌گیری استفاده شد. سپس از روش میدانی برای توزیع پرسشنامه مقایسات زوجی پنج درجه‌ای جهت گردآوری داده‌ها استفاده شد.

پرسشنامه اول برگرفته از ادبیات پژوهش و با بهره‌گیری از تکنیک دلفی، بین ۱۵ نفر از خبرگان توزیع شد. نظرخواهی از گروه خبرگان مطالعه دلفی، به صورت ارسال پرسشنامه ساختار یافته طیف ۵ تایی لیکرت، مشتمل بر ۲۲ سؤال، در طی دو دور با شرکت ۱۵ نفر صورت گرفت، به گونه‌ای که ابتدا پرسشنامه نخست مشتمل بر ۲۲ سؤال بین اعضاء گروه دلفی توزیع و پس از جمع‌آوری پرسشنامه‌های تکمیل شده و ارزیابی نتایج این دور دلفی، ۵ عامل اصلی و ۲۱ زیرعامل حائز اهمیت شناخته شدند (زیرعامل قوانین ومقررات با میانگین ۲/۸۷±۸۳ و مقدار تی ۰/۶۱ حائز اهمیت تشخیص داده نشد و برای دور دوم از پرسشنامه کنار گذاشته شد) و پس از گذشت بیست روز، از نظرخواهی اولیه، عوامل حائز اهمیت، جهت انجام دور بعدی دلفی در قالب یک پرسشنامه ۲۱ سؤالی مربوط به زیرعوامل حائز اهمیت مورد ارزیابی مجدد قرار گرفتند که داده‌های جمع‌آوری شده نشان از تأیید تمام زیرعوامل داشت (جدول ۲ و ۳). در نهایت، داده‌ها به روش تحلیل سلسله مراتبی و با استفاده از نرم‌افزار اکسپرت چویس تجزیه و تحلیل شد.

جدول (۲). نتایج آزمون تی تک نمونه‌ای مربوط به پرسشنامه دور دوم دلفی

عامل اصلی	زیرعامل	میانگین	انحراف معیار	آماره t	سطح معنی‌داری	نتیجه
عوامل فردی عمدی	طمع شخصی	۴/۰۷	۰/۷۹	۵/۱۷	۰/۰۰۰	با اهمیت
	نارضایتی شغلی	۳/۹۳	۰/۷۹	۴/۵۲	۰/۰۰۰	با اهمیت
	گسست اخلاقی	۴	۰/۷۵	۵/۱۲	۰/۰۰۰	با اهمیت
	تجربه تهاجم به حریم خصوصی	۳/۶۰	۰/۶۳	۳/۶۷	۰/۰۰۳	با اهمیت
	حسادت کارکنان	۳/۸۰	۰/۸۶	۳/۵۹	۰/۰۰۰	با اهمیت
	عدم اعتماد کارکنان	۳/۸۰	۰/۶۷	۴/۵۸	۰/۰۰۰	با اهمیت
	عدم انگیزه کارکنان	۳/۸۷	۰/۶۴	۵/۲۴	۰/۰۰۰	با اهمیت
عوامل فردی غیرعمدی	سهل انگاری	۴/۰۷	۰/۷۰	۵/۸۷	۰/۰۰۰	با اهمیت
	عدم پشتیبانی مدیریت ارشد	۳/۹۳	۰/۴۵	۷/۸۹	۰/۰۰۰	با اهمیت
	عدم آموزش مناسب کارکنان	۳/۸۰	۰/۶۷	۴/۵۸	۰/۰۰۰	با اهمیت
	نامشخص بودن حوزه وظایف کاکنان جدید	۴	۰/۵۳	۷/۲۴	۰/۰۰۰	با اهمیت
	استفاده از کارکنان قراردادی و موقتی	۳/۷۳	۰/۹۶	۲/۹۵	۰/۰۱۰	با اهمیت
عوامل محیطی	درخواست اطلاع‌رسانی ذینفعان از حوادث امنیتی	۴	۰/۷۵	۵/۱۲	۰/۰۰۰	با اهمیت
	الزامات نظارتی	۳/۸۷	۰/۶۴	۵/۲۴	۰/۰۰۰	با اهمیت
	الزامات شرکای تجاری	۳/۶۷	۰/۷۲	۳/۵۶	۰/۰۰۳	با اهمیت

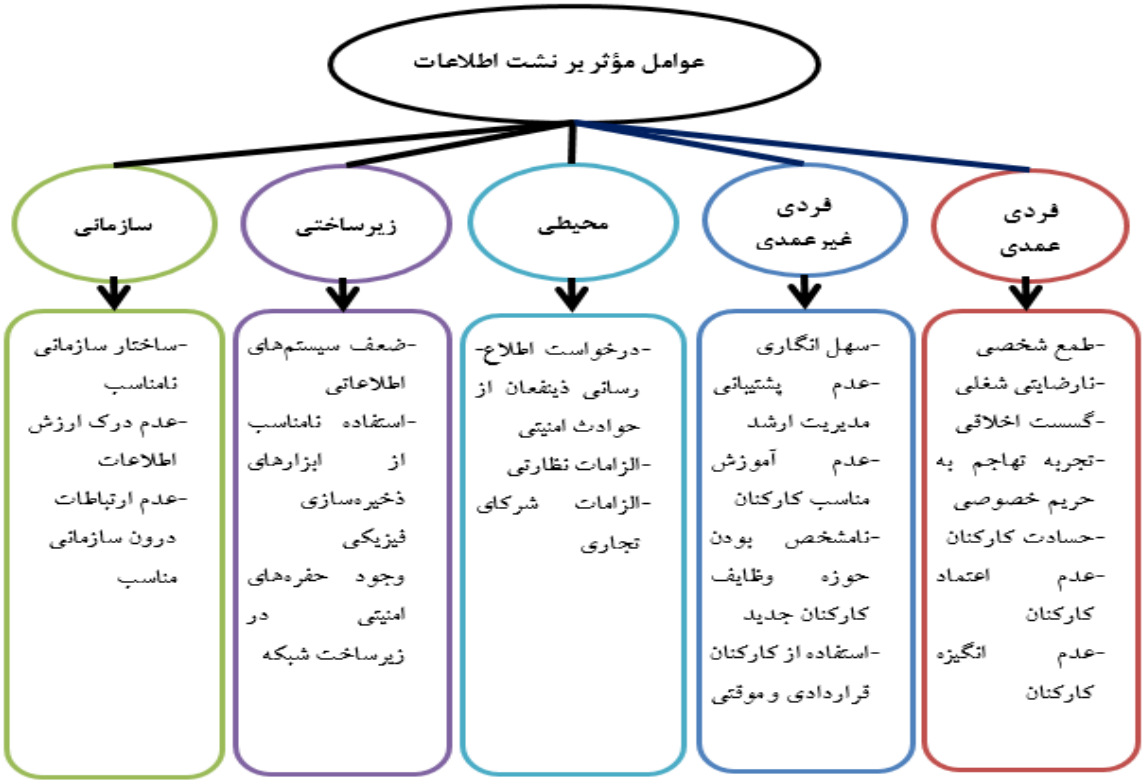
عوامل زیرساختی	ضعف سیستم‌های اطلاعاتی	۳/۹۳	۰/۷۰	۵/۱۳	۰/۰۰۰	با اهمیت
	استفاده نامناسب از ابزارهای ذخیره سازی فیزیکی	۳/۸۰	۰/۶۷	۴/۵۸	۰/۰۰۰	با اهمیت
	وجود حفره‌های امنیتی در زیرساخت شبکه	۳/۶۷	۰/۶۱	۴/۱۸	۰/۰۰۱	با اهمیت
عوامل سازمانی	ساختار سازمانی نامناسب	۳/۸۷	۰/۷۴	۴/۵۱	۰/۰۰۰	با اهمیت
	عدم درک ارزش اطلاعات	۴/۰۷	۰/۷۰	۵/۸۷	۰/۰۰۰	با اهمیت
	عدم ارتباطات درون سازمان مناسب	۳/۸۰	۰/۷۷	۴	۰/۰۰۱	با اهمیت

همان‌طور که در جدول (۲)، مشاهده می‌شود، طبق نظرات خبرگان در دور دوم دلفی، ۵ عامل اصلی و ۲۱ زیرعامل، میانگین نمره بالاتر از ۳ و سطح معناداری آزمون کمتر از ۰/۰۵ را به خود اختصاص دادند، لذا با اعتماد بالای ۹۵ درصد می‌توان نتیجه گرفت، این ۵ عامل اصلی و ۲۱ زیرعامل با اهمیت هستند.

جدول (۳). بررسی نتایج آزمون کندال دور دوم فرایند دلفی

متغیر	تعداد سؤالات	تعداد خبرگان	ضریب هماهنگی کندال	ضریب کای دو	درجه آزادی	میزان خطا (α)	سطح معنی‌داری
بررسی پرسشنامه	۲۱	۱۵	۰/۷۲۳	۱۲۴/۵۳	۱۴	۰/۰۵	۰/۰۰۱

با توجه به نتایج آزمون کندال (جدول ۳) مقدار سطح معنی‌داری در سطح خطای ۰/۰۵ معنی‌دار است که نشان می‌دهد با ۹۵ درصد اطمینان زیرعامل‌ها تأیید شده است و می‌توان از این زیرعامل‌ها جهت اجرای پژوهش استفاده کرد. برای بررسی نوع و شدت رابطه مقدار ضریب هماهنگی اهمیت دارد. با توجه به این‌که شدت ضریب هماهنگی کندال مثبت و مقدار این شدت نیز ۰/۷۲۳ است، بنابراین می‌توان به این نتیجه رسید که این مولفه‌ها جهت اجرای فرایند پژوهش مورد تایید هستند. در پایان از دسته‌بندی زیرعامل‌ها در قالب عامل‌های اصلی درخت تصمیم به شکل زیر ترسیم شد (شکل ۱).



شکل (۱). درخت تصمیم‌گیری پژوهش

یافته‌های پژوهش

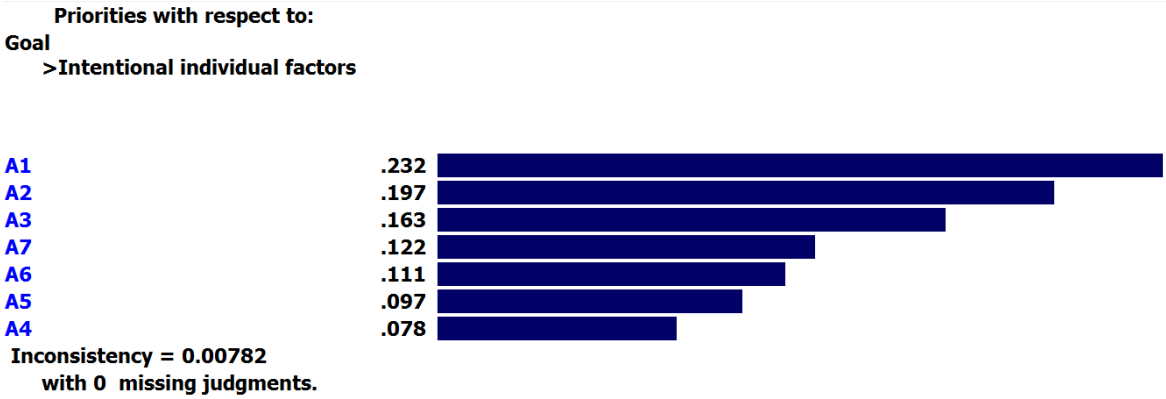
بعد از مشخص شدن ۵ عامل اصلی و دسته‌بندی ۲۱ زیرعامل ذیل عوامل اصلی پنج‌گانه، وزن‌دهی و اولویت بندی عوامل موثر بر نشت اطلاعات انجام شد. نتایج این تحلیل‌ها در سطح عامل‌های اصلی در ادامه ذکر شده است.

وزن و اولویت‌بندی عوامل فردی عمدی

جدول (۴). ماتریس مقایسات زوجی زیرعوامل فردی عمدی

زیرعوامل فردی عمدی	A2	A3	A4	A5	A6	A7
طمع شخصی (A1)	۱/۳۲۵	۱/۵۲۹	۲/۶۱۸	۲/۳۷۴	۲/۱۵۵	۱/۸۵۲
نارضایتی شغلی (A2)		۱/۳۰۵	۲/۴۱۵	۲/۱۵۸	۱/۹۲۵	۱/۶۲۴
گسست اخلاقی (A3)			۲/۰۱۲	۱/۹۲۵	۱/۶۲۶	۱/۳۲۵
تجربه تهاجم به حریم خصوصی (A4)				۱/۹۲۶	۱/۵۰۲	۱/۲۸۵
حسادت کارکنان (A5)					۱/۵۵۶	۱/۳۱۲
عدم اعتماد کارکنان (A6)						۱/۲۷۷
عدم انگیزه کارکنان (A7)						

جدول ۴ نتایج ماتریس مقایسات زوجی برای وزن نسبی زیرعامل‌های فردی عمدی را بر اساس تاثیر بر نشت اطلاعات به عنوان هدف نشان می‌دهد.



شکل (۲). رتبه‌بندی زیرعوامل فردی عمدی با استفاده از نرم‌افزار اکسپرت چویس

نتایج شکل (۲) نشان می‌دهد که زیرعامل «طمع شخصی» با وزن ۰/۲۳۲ بیشترین اهمیت و در اولویت اول و زیرعامل «تجربه تهاجم به حریم خصوصی» با وزن نسبی ۰/۰۷۸ کمترین اهمیت و در اولویت هفتم قرار دارد. نرخ ناسازگاری مقایسات زوجی ۰/۰۰۷۸۲ به دست آمده است که چون کمتر از ۰/۱ است، این مقایسات قابل قبول است.

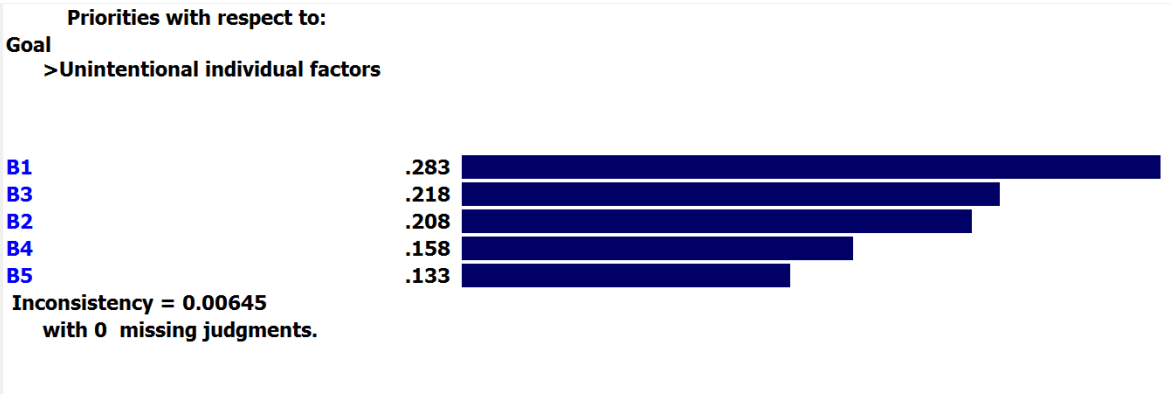
وزن و اولویت‌بندی عوامل فردی غیرعمدی

جدول (۵). ماتریس مقایسات زوجی زیرعوامل فردی غیرعمدی

زیرعوامل فردی غیرعمدی	B2	B3	B4	B5
سهل انگاری (B1)	۱/۵۶۲	۱/۲۹۵	۱/۷۵۲	۱/۹۲۹
عدم پشتیبانی مدیریت ارشد (B2)		۱/۲۸۲	۱/۵۰۴	۱/۸۷
عدم آموزش مناسب کارکنان (B3)			۱/۲۲۲	۱/۴۹۵
نامشخص بودن حوزه وظایف کاکنان جدید (B4)				۱/۲۰۹

استفاده از کارکنان قراردادی و موقتی (B5)

جدول (۵) نتایج ماتریس مقایسات زوجی برای وزن نسبی زیرعامل‌های فردی غیرعمدی را بر اساس تاثیر بر نشت اطلاعات به عنوان هدف نشان می‌دهد.



شکل (۳). رتبه‌بندی زیرعوامل فردی غیرعمدی با استفاده از نرم‌افزار اکسپرت چویس

نتایج شکل (۳) نشان می‌دهد که زیرعامل «سهل انگاری» با وزن ۲۸۳/. بیشترین اهمیت و اولویت نخست و زیرعامل «استفاده از کارکنان قراردادی و موقتی» با وزن نسبی ۰/۱۳۳ کمترین اهمیت و اولویت پنجم را داراست. نرخ ناسازگاری مقایسات زوجی ۰/۰۰۶۴۵ بدست آمده است که چون کمتر از ۰/۱ است، این مقایسات قابل قبول است.

وزن و اولویت‌بندی عوامل محیطی

جدول (۶). ماتریس مقایسات زوجی زیرعوامل محیطی

زیرعوامل محیطی	C2	C3
درخواست اطلاع‌رسان ذینفعان از حوادث امنیتی (C1)	۱/۳۱۲	۱/۵۶۸
الزامات نظارتی (C2)		۱/۲۸۵
الزامات شرکای تجاری (C3)		

جدول (۶) نتایج ماتریس مقایسات زوجی برای وزن نسبی زیرعامل‌های محیطی را بر اساس تاثیر بر نشت اطلاعات به عنوان هدف نشان می‌دهد.

شکل (۴). رتبه‌بندی زیرعوامل محیطی با استفاده از نرم‌افزار اکسپرت چویس

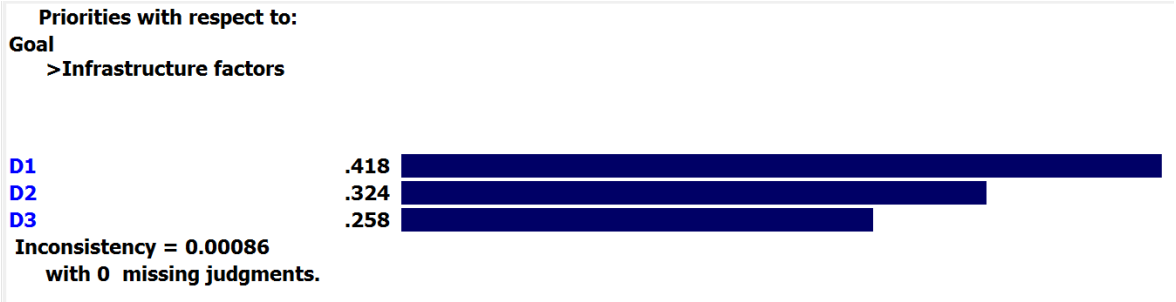
آن‌چه از داده‌های شکل (۴) استنباط می‌شود این که زیرعامل «درخواست اطلاع‌رسانی ذینفعان از حوادث امنیتی» با وزن ۰/۴۱۶ بیشترین اهمیت و در اولویت نخست و زیرعامل «الزامات شرکای تجاری» با وزن نسبی ۰/۲۵۹ کمترین اهمیت و در اولویت سوم قرار دارند. نرخ ناسازگاری مقایسات زوجی ۰/۰۰۰۵۶ بدست آمده است که چون کمتر از ۰/۱ است، این مقایسات قابل قبول است.

وزن و اولویت‌بندی عوامل زیرساختی

جدول (۷). ماتریس مقایسات زوجی زیرعوامل زیرساختی

عوامل زیرساختی	D2	D3
ضعف سیستم‌های اطلاعاتی(D1)	۱/۳۳۳	۱/۵۷۴
استفاده نامناسب از ابزارهای ذخیره‌سازی فیزیکی (D2)		۱/۲۹۲
وجود حفره‌های امنیتی در زیرساخت شبکه (D3)		

جدول (۶) نتایج ماتریس مقایسات زوجی برای وزن نسبی زیرعامل‌های زیرساختی بر اساس تاثیر بر نشت اطلاعات به عنوان هدف نشان می‌دهد.



شکل (۵). رتبه‌بندی زیرعوامل زیرساختی با استفاده از نرم‌افزار اکسپرت چویس

با توجه به شکل (۵) مشاهده می‌شود که زیرعامل «ضعف سیستم‌های اطلاعاتی» با وزن ۰/۴۱۸ بیشترین اهمیت و در اولویت نخست و زیرعامل «وجود حفره‌های امنیتی در زیرساخت شبکه» با وزن نسبی ۰/۲۵۸ کمترین اهمیت و اولویت سوم را داراست. نرخ ناسازگاری مقایسات زوجی ۰/۰۰۰۸۶ بدست آمده است که چون کمتر از ۰/۱ است، این مقایسات قابل قبول است.

وزن و اولویت‌بندی عوامل سازمانی

جدول (۸). ماتریس مقایسات زوجی زیرعوامل سازمانی

زیرعوامل سازمانی	E2	E3
ساختار سازمانی نامناسب (E1)	۱/۲۹۲	۱/۵۰۲
عدم درک ارزش اطلاعات (E2)		۱/۳۱۲
عدم ارتباطات درون سازمان مناسب (E3)		

جدول (۸) نتایج ماتریس مقایسات زوجی برای وزن نسبی زیرعامل‌های فردی عمدی را بر اساس تاثیر بر نشت اطلاعات به عنوان هدف نشان می‌دهد.

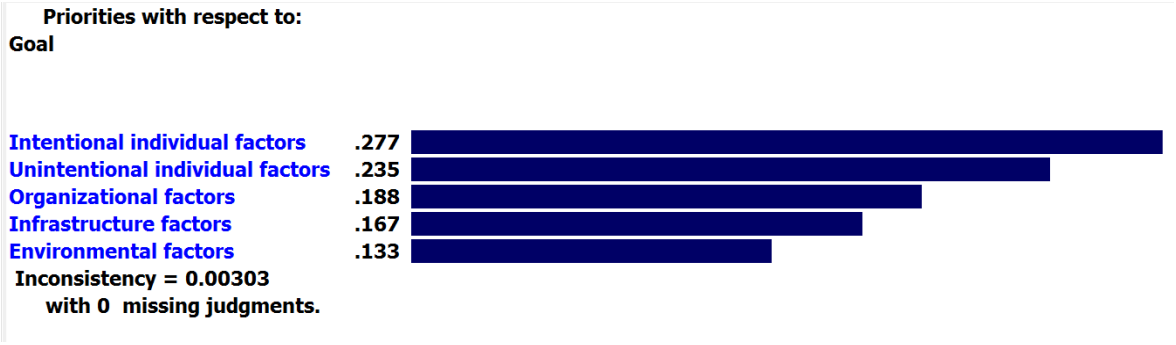
شکل (۶). رتبه بندی زیرعوامل سازمانی با استفاده از نرم‌افزار اکسپرت چویس

با توجه به شکل (۶) مشاهده می‌شود که زیرعامل «عدم درک ارزش اطلاعات» با وزن ۰/۳۹۲ بیشترین اهمیت و در اولویت نخست و زیرعامل «عدم ارتباطات درون سازمانی مناسب» با وزن نسبی ۰/۲۶۲ کمترین اهمیت و در اولویت سوم قرار دارد. نرخ ناسازگاری مقایسات زوجی ۰/۰۲ بدست آمده است که چون کمتر از ۰/۱ است، این مقایسات قابل قبول است. در ادامه وزن و اولویت‌بندی عامل‌های اصلی انجام شد.

جدول (۹). ماتریس مقایسات زوجی عوامل اصلی پژوهش

عوامل سازمانی	عوامل زیرساختی	عوامل محیطی	عوامل غیرعمدی	فردی	عوامل عمدی	فردی	عوامل اصلی
۱/۴۸۵	۱/۶۷۴	۱/۹۲۵	۱/۲۵۲				عوامل فردی عمدی
۱/۲۸۵	۱/۴۹۲	۱/۷۳۶					عوامل فردی غیرعمدی
۱/۳۰۱	۱/۵۰۲						عوامل محیطی
۱/۲۶۵							عوامل زیرساختی
							عوامل سازمانی

جدول (۹) نتایج ماتریس مقایسات زوجی برای وزن نسبی در سطح عامل‌های اصلی را بر اساس تاثیر بر نشت اطلاعات به عنوان هدف نشان می‌دهد.



شکل (۷). رتبه‌بندی عوامل اصلی با استفاده از نرم‌افزار اکسپرت چویس

با توجه به داده‌های شکل (۷) می‌توان گفت که عامل «فردی عمدی» با وزن نسبی ۰/۲۷۷ بیشترین اهمیت و اولویت اول و عامل «محیطی» با وزن ۰/۱۳۳ کمترین اهمیت و اولویت پنجم را دارا می‌باشد. نرخ ناسازگاری مقایسات زوجی ۰/۰۰۳۰۳ بدست آمده است که چون کمتر از ۰/۱۰ است، این مقایسات قابل قبول می‌باشد.

جدول (۱۰). مقایسه وزن نسبی و درصد وزن نهایی هر یک از عوامل و زیرعوامل

عامل	وزن نسبی	زیرعامل	وزن نسبی	درصد وزن نهایی
عوامل فردی عمدی	۰/۲۷۷	طمع شخصی	۰/۲۳۲	۶/۴۳
		نارضایتی شغلی	۰/۱۹۷	۵/۴۶
		گسست اخلاقی	۰/۱۶۳	۴/۵۲
		تجربه تهاجم به حریم خصوصی	۰/۰۷۸	۲/۱۶
		حسادت کارکنان	۰/۰۹۷	۲/۶۹
		عدم اعتماد کارکنان	۰/۱۱۱	۳/۰۷
		عدم انگیزه کارکنان	۰/۱۲۲	۳/۳۸
عوامل فردی	۰/۲۳۵	سهل انگاری	۰/۲۸۳	۶/۶۵
		عدم پشتیبانی مدیریت ارشد	۰/۲۰۸	۴/۸۹

		عدم آموزش مناسب کارکنان	۰/۲۱۸	**۵/۱۲**
		نامشخص بودن حوزه وظایف کاکنان جدید	۰/۱۵۸	**۳/۷۱**
		استفاده از کارکنان قراردادی و موقتی	۰/۱۳۳	**۳/۱۳**
عوامل محیطی	۰/۱۳۳	درخواست اطلاع‌رسانی ذینفعان از حوادث امنیتی	۰/۴۱۶	**۵/۵۳**
		الزامات نظارتی	۰/۳۲۵	**۴/۳۲**
		الزامات شرکای تجاری	۰/۲۵۹	**۳/۴۴**
زیرساختی	۰/۱۶۷	ضعف سیستم‌های اطلاعاتی	۰/۴۱۸	**۶/۹۸**
عوامل		استفاده نامناسب از ابزارهای ذخیره‌سازی فیزیکی	۰/۳۲۴	**۵/۴۱**
		وجود حفره‌های امنیتی در زیرساخت شبکه	۰/۲۵۸	**۴/۳۱**
عوامل سازمانی	۰/۱۸۸	ساختار سازمانی نامناسب	۰/۳۴۶	**۶/۵۰**
		عدم درک ارزش اطلاعات	۰/۳۹۲	**۷/۳۶**
		عدم ارتباطات درون سازمان مناسب	۰/۲۶۲	**۴/۹۳**

وزن نسبی عوامل اصلی و وزن نسبی و درصد وزن نهایی زیرعامل‌ها در جدول (۱۰) آمده است. نتایج جدول نشان می‌دهد که در سطح عوامل اصلی، به ترتیب عوامل فردی عمدی با وزن نسبی ۰/۲۷۷، عوامل فردی غیرعمدی با وزن نسبی ۰/۲۳۵، عوامل سازمانی با وزن نسبی ۰/۱۸۸، عوامل زیرساختی با وزن نسبی ۰/۱۶۷ و عوامل محیطی با وزن نسبی ۰/۱۳۳ در اولویت اول تا پنجم قرار گرفتند. در سطح زیرعامل‌های ۲۱گانه نیز عدم درک ارزش اطلاعات با وزن ۰/۳۹۲ و درصد وزن نسبی ۷/۳۶ در رتبه نخست و تجربه تهاجم به حریم خصوصی با وزن نسبی ۰/۰۷۸ و درصد وزن نسبی ۲/۱۶ در اولویت بیست و یکم قرار گرفتند.

بحث و نتیجه‌گیری

فهم سازمان‌های عصر حاضر از اطلاعات به عنوان یک دارائی مهم، راهبردی و ارزش‌آفرین سبب شده است مدیریت اطلاعات بیش از پیش مورد توجه قرار گیرد و به دنبال بکارگیری سازوکارهایی باشند، تا به تسهیل جریان اطلاعات و اشتراک‌گذاری آن در محیط عملیاتی خود باشند. هرچند این نگاه توسعه‌گرایانه دارای مزایای واضحی برای سازمان‌ها است، اما خطر نشت اطلاعات را به همراه دارد که سازمان‌ها باید از آن آگاه باشند. در پژوهش حاضر به شناسایی و رتبه‌بندی عوامل مؤثر بر نشت اطلاعات سازمانی به روش فرایند تحلیل سلسله مراتبی در فرودگاه بین‌المللی اهواز پرداخته شد. نتایج مطالعه دلفی در دو راند منجر به شناسایی ۵ عامل اصلی و ۲۱ زیرعامل شامل عوامل فردی عمدی (طمع شخصی؛ نارضایتی شغلی؛ گسست اخلاقی؛ تجربه تهاجم به حریم خصوصی؛ حسادت کارکنان؛ عدم اعتماد کارکنان؛ عدم انگیزه کارکنان)، عوامل فردی غیرعمدی (سهل انگاری؛ عدم پشتیبانی مدیریت ارشد؛ عدم آموزش مناسب کارکنان؛ نامشخص بودن حوزه وظایف کارکنان جدید؛ استفاده از کارکنان قراردادی و موقتی)، عوامل محیطی (درخواست ذینفعان در جهت اطلاع‌رسانی در خصوص حوادث امنیتی؛ الزامات نظارتی؛ الزامات شرکای تجاری)، زیرساختی (ضعف سیستم‌های اطلاعاتی؛ استفاده نامناسب از ابزارهای ذخیره‌سازی فیزیکی؛ وجود حفره‌های امنیتی در زیرساخت شبکه، و عوامل سازمانی (ساختار سازمانی نامناسب؛ عدم درک ارزش اطلاعات؛ عدم ارتباطات درون سازمان مناسب) گردید.

بر اساس نتایج بدست آمده، عوامل فردی عمدی با وزن ۰/۲۷۷ اولین عامل مؤثر بر نشت اطلاعات در فرودگاه بین‌المللی اهواز بودند. هم‌چنین در بین زیرعوامل فردی عمدی، طمع شخصی با وزن ۰/۲۳۲ با اهمیت‌ترین زیرعامل و تجربه تهاجم به حریم خصوصی با وزن ۰/۰۷۸ کم اهمیت‌ترین زیرعامل بود. یافته‌ها تأیید کرد که نشت عمدی اطلاعات به دلیل عوامل انسانی هنوز هم بایستی مورد توجه مدیران باشد. از آن‌جا که کنار گذاشتن عوامل انسانی در چرخه حیات سازمانی اطلاعات در عمل امکان‌پذیر نیست، مدیران بایستی این چالش را پذیرفته و به دنبال سازوکارهای مناسب با آن باشند. به عبارت دیگر با وجود عوامل انسانی، سازمان‌ها با چالش نشت عمدی یا غیرعمدی اطلاعات مواجه می‌شوند. ممکن است نشت عمدی اطلاعات در سازمان به دلیل طمع شخصی در مقابل منافع سازمانی اتفاق افتاد که در آن کارکنان مایلند اطلاعات سازمان را

به دلایل مادی به رقبا بفروشند و منافع خود را بر منافع سازمان ترجیح دهند. حسادت کارمند شرکت به همکاران یا کارکنان شرکت‌های رقیب، ناراضی بودن از شرکت یا احساس کینه توزی به هر دلیلی نیز باعث نشت عمدی اطلاعات می‌شود. کارمندان ناراضی نیز ممکن است عمداً اطلاعات مهم را در اختیار اشخاص غیرمجاز قرار دهند. از سوی دیگر بر اساس برخی مطالعات، افراد ممکن است نگرانی‌های متفاوتی در مورد حریم خصوصی خود داشته باشند. با این حال، معمولاً، نقض حریم خصوصی ناشی از تجربیات منفی، مانند نشت داده یا سرقت، به دلیل ترس از تکرار تجربه منفی ممکن است رخ دهد. یکی از عوامل بروز رفتارهای نابهنجار سازمانی عدم اعتماد است. این عدم اعتماد می‌تواند دارای زمینه فردی، سازمانی و خارجی باشد. اگر کارکنان دچار عدم اعتماد شوند به راحتی قادر به بروز رفتارهای منفی بر علیه سیاست‌های سازمان به خصوص نشت اطلاعات خواهند شد. عدم انگیزه برای رعایت سیاست‌های امنیت اطلاعات عامل مؤثری در جهت خروج اطلاعات از سازمان خواهد بود. بر اساس نظریه انتظار، افراد شیوه رفتاری‌شان را بر مبنای نتایجی انتخاب می‌کنند که انتظار دارند از رفتارشان به دست آورند. اگر افراد انگیزه مناسبی برای محیط کار نداشته باشند به سمت رفتارهای انحرافی کشیده خواهند شد. علاوه بر این، برخی سازمان‌ها با هکرهای خودی مخربی روبرو هستند که به دلیل قوانین ناکافی حفاظت از داده‌ها، اطلاعات ارزشمند شرکت را نقض می‌کنند. از این رو، تمام رفتارهای عمدی انسان، اقداماتی بر پایه گسست‌های اخلاقی برای آسیب رساندن به امنیت و عملیات تجاری هستند. گسست اخلاقی مکانیسمی است که از طریق آن افراد به طور ذهنی پیامدهای رفتارهای ناخواسته را از ارزش‌های اخلاقی خود کاهش می‌دهند. یافته‌های مطالعه در این بخش با بخشی از نتایج مطالعات قبلی مانند وونگ و همکاران (۲۰۲۰)؛ مغول (۲۰۲۱) و کاپلوزا و همکاران (۲۰۲۲) همسو است.

براساس نتایج عوامل فردی غیرعمدی نیز با وزن ۰/۲۳۵ دومین عامل مؤثر بر نشت اطلاعات در فرودگاه بین‌المللی اهواز بودند. هم‌چنین در بین زیرعوامل فردی غیرعمدی، سهل انگاری با وزن ۰/۲۸۳ با اهمیت‌ترین زیرعامل و استفاده از کارکنان قراردادی و موقتی با وزن ۰/۱۳۳ کم اهمیت‌ترین زیرعامل بود. نشت غیرعمدی زمانی اتفاق می‌افتد که یک شخص داخلی به طور ناخواسته اطلاعات مهم تجاری را که قرار نیست با اشخاص ثالث به اشتراک گذاشته شود، افشا می‌کند (ریتالا، اولاندر، میچایلووا و هاستد، ۲۰۱۵؛ تان و همکاران، ۲۰۱۶). تهدید فردی غیرعمدی، بالقوه رفتار فردی است که از طریق اقدام یا عمل تصادفی، بدون قصد مخرب، به شبکه، سیستم یا داده‌های یک سازمان دسترسی مجاز داشته، و باعث آسیب یا افزایش قابل ملاحظه احتمال آسیب جدی در آینده به محرمانه بودن، یکپارچگی یا ارزش اطلاعات سازمان شود (گریتزر، استروزر، کوهن، برگی، کاولی، مور و موندی، ۲۰۱۴؛ گریتزر، استروزر، کوهن، مور، موندی و کاولی، ۲۰۱۴). گاهی نشت غیرعمدی به این دلیل رخ داد که کارکنان به دلیل سهل انگاری وظایف خود را برای محافظت از خود زیر پا می‌گذارند و به طور تصادفی اطلاعات ارزشمند را به طرف‌های خارجی نشت می‌دهند. به دلبل آموزش نامناسب کارکنان در مورد رفتارهای مخاطره آمیز نیز ممکن است به طور تصادفی اطلاعات درز کند. گاهی نیز افشای غیرعمدی به دلیل کارمندان جدیدی باشد که به دلیل نامشخص بودن حوزه کاری و آن‌چه که واقعاً باید انجام دهند اطلاعات ارزشمند را برای شرکا افشا کنند. عدم پشتیبانی مدیریت ارشد نیز می‌تواند زمینه‌ساز بروز رفتارهای انحرافی باشد. استفاده از کارکنان قراردادی و موقتی ممکن است منجر به نشت اطلاعات سازمانی گردد. این افراد به دلیل تعهد سازمانی پایین و یا اخراج از محیط کار ممکن است به سمت شرکت‌ها رقیب رفته و اطلاعات سازمان را در اختیار آنها قرار دهند. سازمان‌ها باید در هنگام استخدام توجه بیشتری در زمینه جذب نیروی انسانی داشته باشند و با بستن قراردادهای طولانی مدت و اجتناب از استخدام دوره‌ای از این عامل مؤثر بر نشت اطلاعات بکاهند. بنابراین، خطای انسانی منبع مهمی است که ممکن است به دارایی‌های اطلاعاتی آسیب برساند یا از بین ببرد. یافته‌های مطالعه در این زمینه با بخشی از نتایج مطالعات گذشته مانند محمد وهمکاران (۲۰۰۶)؛ عبدالملوک و همکاران (۲۰۱۰)؛ وونگ و همکاران (۲۰۲۰)؛ هاداش و همکاران (۲۰۱۲)؛ و تان و همکاران (۲۰۱۶) همسو است.

بر اساس نتایج بدست آمده، عوامل سازمانی با وزن ۰/۱۸۸ سومین عامل مؤثر بر نشت اطلاعات در فرودگاه بین‌المللی اهواز بودند. هم‌چنین در بین زیرعوامل سازمانی، عدم درک ارزش اطلاعات با وزن ۰/۳۹۲ با اهمیت‌ترین زیرعامل و عدم ارتباطات درون سازمانی مناسب با وزن ۰/۲۶۲ کم اهمیت‌ترین زیرعامل بود. اولین مورد عدم درک ارزش اطلاعات است. کارکنان بسته

به سطح سلسله مراتبی، نوع اطلاعات و نوع ساختار سازمانی، اطلاعات را متفاوت ارزیابی می‌کنند. ادراک کارکنان از ارزش اطلاعات توسط پژوهش‌گران مختلف به عنوان یک جنبه مهم توصیف می‌شود. این عدم آگاهی منجر به این می‌شود که ارزش اطلاعات مشخص نباشد، لذا پیامدهای منفی ناشی از نشت اطلاعات نیز توسط آنان جدی گرفته نشود. دومین مورد ساختار سازمانی نامناسب است. شرکت‌های بزرگ به صورت طولانی مدت نسبت به حفاظت از داده‌ها حساس هستند. شرکت‌های کوچک‌تر از چنین آگاهی گسترده‌ای برخوردار نیستند. به طور کلی ساختار سازمانی از نظر رسمیت و مکانیسم‌های کنترل موجود ممکن است بر نشت اطلاعات تأثیر بگذارد. سومین مورد عدم ارتباطات درون سازمانی مناسب است. برای دستیابی به درک مشترک، ارتباطات برای انتقال مجموعه‌ای از ارزش‌ها و هنجارهای لازم که قوانین یا زمینه تعامل را تعریف می‌کند، مورد نیاز است. هنجارها بر رفتارهای بعدی کارکنان تأثیر می‌گذارند و می‌توانند به عنوان مکانیسم‌های کنترل رسمی، که معمولاً در قالب قوانین و رویه‌ها مدون شده‌اند، یا از طریق تأثیر همتایان و ساخت اجتماعی واقعیت اعمال شوند. در یک محیط سازمانی، رویکردهای کنترل رسمی و اجتماعی، انتظارات و مرزهای رفتارهای مناسب را برای افراد سازمان تعیین می‌کند. یافته‌های مطالعه از این منظر با بخشی از نتایج پژوهش هاداش و همکاران (۲۰۱۲) همسو است.

هم‌چنین، بر اساس نتایج بدست آمده، عوامل زیرساختی با وزن ۰/۱۶۷ چهارمین عامل مؤثر بر نشت اطلاعات در فرودگاه بین‌المللی اهواز بودند. به همین ترتیب، در بین زیرعوامل زیرساختی، ضعف سیستم‌های اطلاعاتی با وزن ۰/۴۱۸ با اهمیت‌ترین زیرعامل و وجود حفره‌های امنیتی در زیرساخت شبکه با وزن ۰/۲۵۸ کم اهمیت‌ترین زیرعامل بود. اولین مورد ضعف سیستم‌های اطلاعاتی است. خرید سیستم اطلاعات ناقص و ضعف طراحی سیستم‌های اطلاعاتی ممکن است مشکلات جدی را برای سازمان‌ها ایجاد کند. ساز و کارهایی که خودی‌ها از آن برای انجام وظایف کسب و کار بر اساس سیستم‌های اطلاعاتی معمول خود استفاده می‌کنند می‌توانند برای سرقت دارایی‌های اطلاعاتی نیز مورد استفاده قرار گیرند. برای جلوگیری از نشت و سرقت اطلاعات، باید از ساز و کارها و اقدامات حفاظتی در برابر این روش‌ها استفاده کرد. دومین مورد استفاده نامناسب از ابزارهای فیزیکی ذخیره‌سازی اطلاعات (درایوهای سخت، یو. اس. بی، سی. دی و ...) است. این روزها اکثر اطلاعات داخل سازمان به صورت الکترونیکی ذخیره می‌شوند، رسانه‌های این اطلاعات درایوهای سخت، درایوهای سی. دی و یو. اس. بی‌ها و غیره) ابزارهای فیزیکی هستند که احتمال سرقت فیزیکی آنها وجود دارد. جلوگیری از نشت با این وسایل نیازمند پیاده‌سازی اقدامات امنیتی فیزیکی است. سومین مورد وجود حفره‌های امنیتی در زیرساخت شبکه است. شبکه‌های سازمان، یکی از قسمت‌های ضروری از زیرساخت‌های فناوری اطلاعات سازمان است. در شبکه چندین نوع از ارتباطات وجود دارد. ارتباطات داخل به خارج، در برگیرنده هر گونه ارتباطی است که در داخل مرزهای سازمان آغاز شده و مقصدش خارج از سازمان است. اینها معمولاً گستره وسیعی از خدمات را دربر می‌گیرند که کارکنان برای ارتباط با جهان خارج مورد استفاده قرار می‌دهند. ارتباطات داخل به داخل، تمام ارتباطاتی را که در داخل شبکه سازمان اتفاق می‌افتد پوشش می‌دهد. با این که این نوع ارتباطات معمولاً نشت اطلاعات را نه تولید کرده و نه افزایش می‌دهد، اطلاعاتی که توسط این ساز و کارها انتقال داده می‌شود می‌تواند به دریافت کنندگان غیرمجاز در داخل سازمان ارسال شود و نشت اطلاعاتی را در داخل سازمان به وجود آورد. ارتباطات خارج به داخل، هر ارتباطی را که خارج از سازمان آغاز شده و مقصد آن نقطه‌ای در داخل زیرساخت شبکه سازمان است، پوشش می‌دهد. این نوع ارتباطات، مستعد تولید نشت اطلاعات است، چرا که ممکن است اطلاعات حساس، به اشتباه بر روی یک سرور دسترسی عمومی قرار گیرد. این نتیجه همسو با نتایج پژوهش حسن‌نیا و دهقانی (۱۳۹۲) است.

در انتها، بر اساس نتایج بدست آمده، عوامل محیطی با وزن ۰/۱۳۳ پنجمین عامل مؤثر بر نشت اطلاعات در فرودگاه بین‌المللی اهواز بودند. هم‌چنین در بین زیرعوامل محیطی، درخواست ذینفعان در جهت اطلاع‌رسانی در خصوص حوادث امنیتی با وزن ۰/۴۱۶ با اهمیت‌ترین زیرعامل و الزامات شرکای تجاری با وزن ۰/۲۵۹ کم اهمیت‌ترین زیرعامل بود. یکی از منابع ورودی که رفتار افراد یک سازمان را شکل می‌دهد، محیط سازمانی است. تصمیمات کارکنان تحت تأثیر ساختار محیطی، در دسترس بودن اطلاعات محیطی و معنای مربوطه‌ای است که کارکنان به اطلاعات محیطی اختصاص می‌دهند. اولین مورد درخواست ذینفعان در جهت اطلاع‌رسانی در خصوص حوادث امنیتی است. در دوره اخیر درخواست برای نوع رخدادهای نشت اطلاعات برای شرکت‌ها شدیدتر است، ذینفعان بیرونی و داخلی به طور مداوم نگران حفظ یک تصویر عمومی خوب سازمان هستند.

به صورت کلی به نظر می‌رسد علاقه عمومی به حوادث نشت اطلاعات بر سازمان‌ها فشار وارد می‌کند در حالی که واکنش سازمان‌ها پویا است و به نظر می‌رسد در طول زمان تغییر می‌کند. اگر انتظارات ذینفعان نادیده گرفته شود و اجازه داده شود که نفوذ اجتماعی مسیر خود را طی کند، فشار سیاسی و قانونی ایجاد می‌شود که اغلب منجر به پیامدهای منفی شرکت می‌شود. نارضایتی ذینفعان زمانی ایجاد می‌شود که اقدامات شرکتی انتظارات اجتماعی را برآورده نمی‌کند و شکاف بین اقدامات شرکت و انتظارات ذینفعان با کاهش اعتماد عمومی افزایش می یابد. بنابراین هرچه درک کارکنان از حفاظت از اطلاعات به عنوان انتظارات اجتماعی بیشتر باشد، درک بیشتر رویدادهای نشت عمومی به عنوان تهدیدی برای وجهه شرکت خواهد بود. هم‌چنین هرچه درک کارکنان از تصویر خوب به عنوان مزیت رقابتی بیشتر باشد، درک رویدادهای نشت عمومی به عنوان تهدیدی برای تصویر شرکت بالاتر می‌رود (هاداش و همکاران، ۲۰۱۲). مورد بعدی الزامات نظارتی است. علاوه بر انتظارات عمومی تحمیل شده از بیرون، سازمان‌ها با مقررات نهادی ناهمگونی روبرو هستند. هر چه کارکنان درک بیشتری از نحوه اعمال مقررات در مورد نوع اطلاعات در حال پردازش داشته باشد، درک رویدادهای نشت عمومی به عنوان یک تهدید تحریمی بالاتر خواهد بود. مورد سوم نیز الزامات شرکای تجاری است. در زمان تدوین اهداف و کارها، اطلاعات مربوط به مشتریان، تأمین کنندگان و رقبا و به صورت کلی الزامات شرکای تجاری باید توسط افراد سازمان در نظر گرفته شوند. سطح محرمانه بودن در این زمان باید تعیین شود. شدیدترین حادثه نشت از بین رفتن اطلاعات شرکای تجاری خواهد بود. اگر اطلاعات این شرکا در مطبوعات یا جای دیگری منتشر شود، مشتریان قراردادها را لغو کرده و همکاری را متوقف کنند. این نتیجه همسو با نتایج پژوهش هاداش و همکاران (۲۰۱۲) است.

به طورکلی، نتایج نشان می‌دهد که نشت اطلاعاتی یک دغدغه اساسی برای سازمان‌ها است. در این زمینه هرچقدر سازمان به دارائی‌های اطلاعاتی وابستگی بیشتری داشته باشد، دغدغه نشت اطلاعات نیز بیشتر موضوعیت می‌یابد. در چنین شرایطی ذائقه رقبا نیز بیش از پیش تحریک می‌شود که با دستیابی به اطلاعات سازمان، ضمن آگاهی از برنامه‌های سازمان مربوطه، سازوکار لازم را برای مقابله با آن بیاندیشند. از این رو، شناسایی عوامل موثر بر نشت اطلاعات در قالب ۲۱ زیرعامل در ۵ گروه بینش لازم را در اختیار مدیران فرودگاه اهواز قرار داد تا نسبت به تقویت نقاط آسیب‌زا با اتخاذ تدابیر لازم از قبیل اعتمادآفرینی، تقویت حس همکاری، رعایت اخلاق حرفه‌ای، استفاده از اقدامات انگیزشی، آگاهی‌سازی از ارزش اطلاعات، آموزش مناسب کارکنان در خصوص امنیت اطلاعات، بازطراحی سیستم‌های اطلاعاتی و طراحی برنامه هدفمند در خصوص ذخیره‌سازی، اشتراک و انتقال اطلاعات اقدام کنند.

ملاحظات اخلاقی

پیروی از اصول اخلاق پژوهش

این پژوهش برگرفته از یافته‌های پایان‌نامه کارشناسی ارشد مصوب دانشگاه آزاد اسلامی واحد اهواز است. ضمن این که، نویسندگان اصول اخلاقی را در انجام و انتشار این پژوهش علمی رعایت نموده‌اند و این موضوع مورد تأیید همه آن‌هاست.

مشارکت نویسندگان

مشارکت نویسندگان در مقاله مستخرج از پایان‌نامه تقریباً به شکل زیر است:

عبدالامیر مبهوت: گردآوری داده‌ها، انجام محاسبات، تجزیه و تحلیل آماری داده‌ها، تحلیل و تفسیر اطلاعات و نتایج، تهیه پیشنویس مقاله.

محمدرضا فرهادپور: استاد راهنمای پایان‌نامه، طراحی پژوهش، نظارت بر مراحل انجام پژوهش، بررسی و کنترل نتایج، اصلاح، بازبینی و نهایی‌سازی مقاله.

ابراهیم حسینی: مشارکت در طراحی پژوهش، نظارت بر تحلیل داده‌ها، مطالعه و بازبینی مقاله.

تعارض منافع

بنا بر اظهار نویسندگان در خصوص انتشار مقاله حاضر، هیچ‌گونه تعارض منافعی وجود ندارد.

حامی مالی

حمایت مالی از این پژوهش از طرف دانشگاه آزاد اسلامی واحد اهواز دانشکده علوم انسانی در قالب حمایت از پایان‌نامه دانشجویی نویسنده اول انجام شده است.

سپاسگزاری

از معاونت محترم پژوهشی دانشگاه آزاد اسلامی واحد اهواز و فرودگاه اهواز به خاطر حمایت‌های مالی، معنوی و همکاری در اجرای پژوهش حاضر سپاسگزاری می‌شود.

هم‌چنین از ارکان فصلنامه تعامل انسان و اطلاعات و داوران محترم به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.

نگارندگان بر خود لازم می‌دانند از خانم دکتر سمیرا دانیالی به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

اسمعیلی، مریم؛ کفشیان اهر، هاجر. (۱۳۹۸). به اشتراک‌گذاری اطلاعات، نشت اطلاعات و تحریف اطلاعات در یک زنجیره تأمین غیرمتمرکز با یک تولیدکننده و دو خرده‌فروش رقیب. *نشریه پژوهش‌های مهندسی صنایع در سیستم‌های تولید*، ۷(۱۴)، ۱۳-۲۷.

حسن‌نیا، محمد حسین؛ دهقانی، مهدی. (۱۳۹۲). بررسی روش‌های نشت اطلاعات و راه‌کارهای جلوگیری از آن. *فصلنامه پدافند غیرعامل*، ۴(۴)، ۱-۱۲.

صادقی، امیرعباس؛ رزاقی، حمید و احمدی، ثریا. (۱۴۰۲). تعیین مقوله‌های موثر بر نقض حریم خصوصی کاربران در شبکه اجتماعی اینستاگرام. *پایاشهر*، ۵: ۵۷.

طالش، عاطفه؛ فراهی، احمد. (۱۳۹۵). بررسی روش های پیشگیری از نشت اطلاعات. *کنفرانس بین‌المللی پژوهش در علوم و مهندسی*، ۱-۸.

لشگری، سیامک؛ احمدی آبکناری، فاطمه. (۱۳۹۸). توسعه و دسته‌بندی قوانین حفظ حریم خصوصی کاربران در شبکه‌های اجتماعی بر حسب نوع نشت اطلاعات، *کنفرانس ملی آینده پژوهی، مدیریت و توسعه پایدار*، تهران، ۱-۱۳.

نگهدار، ایرج؛ پورقهرمانی، بابک و بیگی، جمال. (۱۴۰۲). سیاستگذاری جنایی در نقض امنیت سایبری و رهیافت‌های پیشگیری اجتماعی. *فصلنامه سیاستگذاری عمومی*، ۹(۲) ۹۶- ۱۱۴.

References

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2010). *Understanding the factors of information leakage through online social networking to safeguard organizational information*, 1-17.

Abdul Molok, N. N., Chang, S., & Ahmad, A. (2013). Disclosure of organizational information on social media: Perspectives from security managers, *PACIS 2013 Proceedings*. 108.

Anand, K. S., & Goyal, M. (2009). Strategic information management under leakage in a supply chain. *Management Science*, 55(3), 438-452.

Bloodgood, J. M., & Chen, A. N. (2021). Preventing organizational knowledge leakage: the influence of knowledge seekers' awareness, motivation and capability. *Journal of Knowledge Management*, 1-32.

Bouke, M. A., Abdullah, A., Udzir, N. I., & Samian, N. (2024). Overcoming the Challenges of Data Lack, Leakage, and Dimensionality in Intrusion Detection Systems: A Comprehensive Review. *Journal of Communication and Information Systems*, *39*(1). https://doi.org/10.14209/jcis.2024.3.

Cappellozza, A., de Moraes, G. H. S. M., Perez, G., & Simões, A. L. (2021). Antecedent factors of violation of information security rules. *RAUSP Management Journal*, 2531-0488.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), e1211.

Dolezel, D., Beauvais, B., Stigler Granados, P., Fulton, L., & Kruse, C. S. (2023). Effects of Internal and External Factors on Hospital Data Breaches: Quantitative Study. *Journal of Medical Internet Research, 25*, e51471. doi: 10.2196/51471

Esmaeili, M. & Kafshian Ahar, H. (2019). Information sharing, information leakage and information distortion in a decentralized supply chain with one manufacturer and two competing retailers. *Journal of Industrial engineering Research in Production Systems*. 7(14): 13-27. Doi: 10.22084/ier.2019.14110.1642. (Persian)

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. *In 2014 IEEE Security and Privacy Workshops*, 236-250.

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014). Unintentional insider threat: contributing factors, observables, and mitigation strategies. *In 2014 47th Hawaii International Conference on System Sciences* (pp. 2025-2034). IEEE.

Hadasch, F., Mueller, B., & Maedche, A. (2012). *Exploring Antecedent Environmental and Organizational Factors to User-Caused Information Leaks: A Qualitative Study*, 127.

Hasan Nia, M. H. & Dehghani, M. (2013). Examining the methods of information compromise and its countermeasures techniques. *Inactive Defense Magazine*, 4(4): 1-12. (Persian).

Jašari, A. (2015). Information systems at the airport. *PROCEEDING BOOK*, 8. Retrieved from: https://icesos.ibu.edu.ba/wp-content/uploads/2019/02/PROCEEDING-BOOK_V41.10.2015-min.pdf#page=8

Kim, S.-H., Kim, N.-U., & Chung, T.-M. (2015). Study on sensitive information leakage vulnerability modeling. *Kybernetes*, 44(1), 77-88.

Lashghari, S. & Ahmadi Abkenari, F. (2019). Development and classification of user privacy rules in social networks according to the type of information leakage. *National Conference on Future Studies, Management and Sustainable Development*. Ghazvin (November 2019), Imam Khomeini International University. (Persian)

Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: identification of key factors affecting data breach incidents. *Humanities and Social Sciences Communications*, *10*(1), 1-18. Retrieved from: https://doi.org/10.1057/s41599-023-01757-0

Madnick, S. E. (2023). The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase.

Martel, N., & Seneviratne, P. N. (1990). Analysis of factors influencing quality of service in passenger terminal buildings. *Transportation Research Record*, (1273).

Mughal, Y. H. (2021). Impact of Supply Chain Information Integration on Operational Performance of Pharmaceutical Firms: Mediating Role of Information Leakage. *Journal of Pharmaceutical Research International*, 33(41B), 69-78.

Negahdar, E., pourghahramani, B., & Beigi, J. (2023). Criminal Policy making in Cyber Security Violations and Social Prevention Approaches. *Iranian Journal of Public Policy*, *9*(2), 97-114. doi: 10.22059/jppolicy.2023.93610

Purnell, J. (2012). *Information technology systems at Airports: A Primer* (Vol. 59). Transportation Research Board.

Rauscher, F., Kogler, A., Juffinger, J., & Gruss, D. (2024, February). IdleLeak: Exploiting Idle State Side Effects for Information Leakage. In *Network and Distributed System Security (NDSS) Symposium 2024*. Retrieved from: https://www.ndss-symposium.org/wp-content/uploads/2024-78-paper.pdf.

Rogers, Z., Benjamin, V., & Gopalakrishnan, M. (2018). *Cyber security in supply chains: Understanding threats and potential security practices. Report.* Center for Advanced Procurement Strategy, Tempe, AZ.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation*, 35, 22-31.

Sadeghi, A., Razaghi, H. & Ahmadi, S. (2023). Determining the factors affecting users' privacy in the Instagram social network. Paya Shahr, 5: 1-23. https://civilica.com/doc/1891414

Schultz, M., Schulz, C., & Fricke, H. (2007, December). Enhanced information flow and guidance in airport terminals using best passenger‘s visual perception. In *Eurocontrol INO Workshop*.

Talesh, A. & Farahi, A. (2016). Investigating methods to prevent information leakage. In: *International Congress on Engineerin Innovation & Technology Development (ICEITD)*. Tabriz (19 May 2016) Tabriz University. (Persian)

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and knowledge leakage in supply chain. *Information Systems Frontiers*, 18(3), 621-638.

Tran, T. T. H., Childerhouse, P., & Deakins, E. (2016). Supply chain information sharing: challenges and risk mitigation strategies. *Journal of Manufacturing Technology Management*, 27(8), 1102-1126.

van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Computers & Security*, 97, 101970.

Wong, W. P., Tan, K. H., Chuah, S. H. W., Tseng, M. L., Wong, K. Y., & Ahmad, S. (2020). Information sharing and the bane of information leakage: a multigroup analysis of contract versus noncontract. *Journal of Enterprise Information Management.*

Wong, W. P., Tan, K. H., Govindan, K., Li, D., & Kumar, A. (2021). A conceptual framework for information-leakage-resilience. *Annals of Operations Research*, 1-21.

Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M. L. (2019). Human factors in information leakage: mitigation strategies for information sharing integrity. *Industrial Management & Data Systems*, *119*(6), 1242-1267.

Wong, W.P., Tan, H.C., Tan, K.H., & Tseng, M. (2020). Human factors in information leakage: mitigation strategies for information sharing integrity. *Ind. Manag. Data Syst.*, 119, 1242-1267. www.dictionary.cambridge.org.